

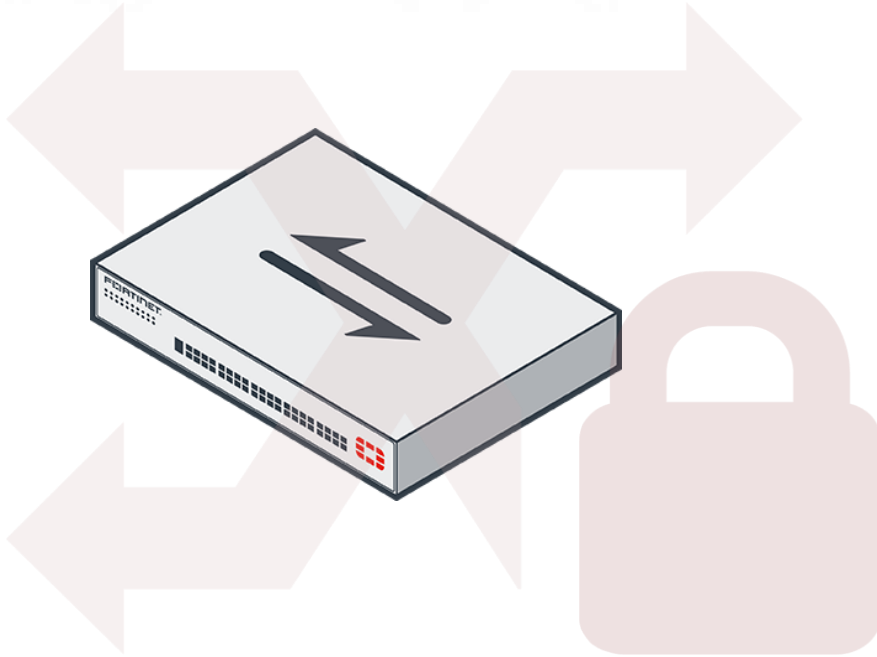
# FortiSwitch Secure Switching

Extending Fortinet Security Fabric to the Access

Q3 2018

# Secure Unified Access Ethernet

## FortiSwitch



### Integrated Security

Pervasive Security through Fortinet Security Fabric Integration addressing the broadest threat surface.

### Simplified Management

FortiGate integration creates one interface to manage security and access.

### Scalable

Able to scale from desktop to datacenter across platforms allowing flexibility to grow as devices and traffic increase.

FortiSwitch becomes a logical extension of the FortiGate when connected via FortiLink

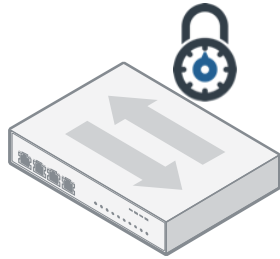
# KEY BENEFITS

## ZERO-TOUCH PROVISIONING



- Easy deployment in high scale
- No login to the switches
- Auto Discovery of Switches

## SECURE AND CENTRALIZED CONFIGURATION MANAGEMENT



- FortiGate is Single Point of Management
- Centralized VLAN and Features provisioning

## SECURITY FABRIC INTEGRATION



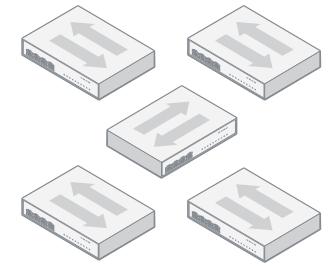
- Device Discovery
- Centralized Authentication
- Host Quarantine
- Dynamic VLAN Assignment
- Logging

## FORTISWITCH STACK



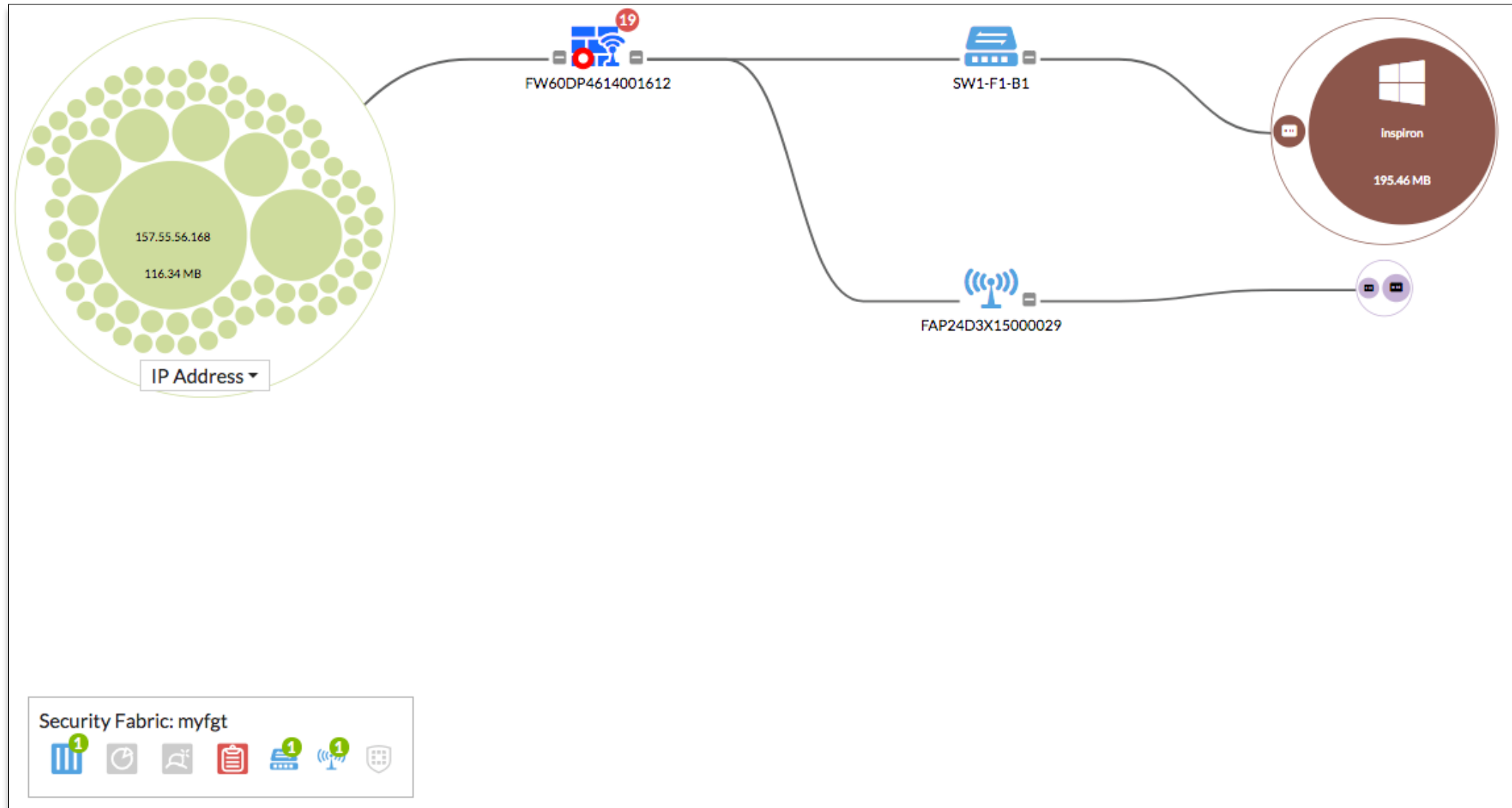
- Stack of FortiSwitches Controlled by FortiGate (Single or HA-Pair)
- MCLAG for loop-free link and switch level redundancy

## MODEL RANGE



- Range of FortiSwitch and FortiGate Models for
  - » Retail
  - » SMB
  - » Enterprise
  - » Datacenter

# FortiSwitch in Fortinet Security Fabric

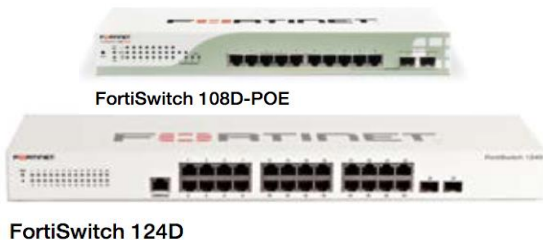


# FortiSwitch Access Switch Family

## Entry

### 100 Series

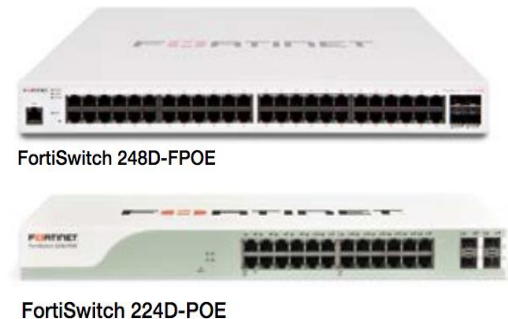
- Entry Level Switch
- 8 to 24 gigabit Ethernet ports, POE Capable
- Desktop to wiring closet.
- (2) Gigabit Ethernet SFP uplink ports



## Mid Range

### 200 Series

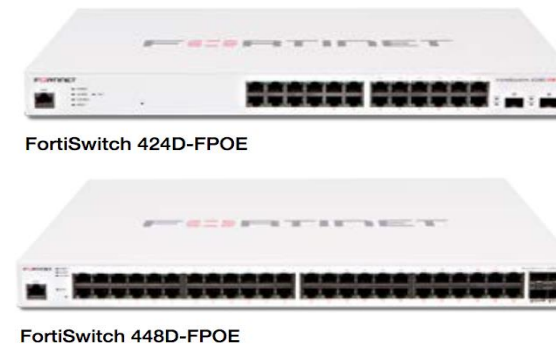
- Mid level Switch
- 24 to 48 gigabit Ethernet ports POE+ Capable
- Typical wiring closet switch
- (4) Gigabit Ethernet SFP uplink ports



## Premium

### 400 Series

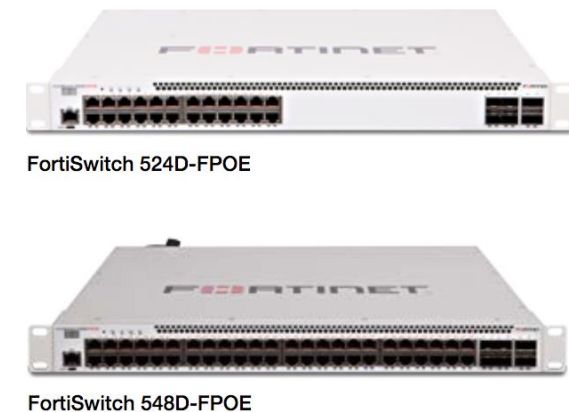
- Enterprise Switch
- 24 to 48 gigabit Ethernet ports POE+ Capable
- Larger wiring closet or high throughput requirements.
- Up to (4) 10 Gigabit Ethernet SFP uplinks



## Aggregation

### 500 Series

- Aggregation Switch
- 24 to 48 gigabit Ethernet ports POE+ Capable
- Up to (4) 10 Gigabit Ethernet (2) 40 Gigabit Ethernet SFP uplinks





# FortiSwitch Top of Rack Aggregation Switch Family

## 1000 Series

- Data Center Aggregation Switch
- 24 or 48 10 Gigabit Ethernet SFP ports
- 1000 Series offers up to **six 40 or four 100 Gigabit** Ethernet QSFP+ uplink ports
- Dual hot swappable power supplies



FortiSwitch 1048D — front



FortiSwitch 1048D — back



FortiSwitch 1024D — front



FortiSwitch 1024D — back

## 3000 Series

- Data Center Switch
- 3000 series offers 32 x 40 Gigabit Ethernet QSFP+ ports
- Dual hot swappable power supplies



FortiSwitch 3032D — front



FortiSwitch 3032D — back

# FortiSwitch Rugged Switch Family

- Rugged Access Switch
- 12 or 24 gigabit Ethernet ports
- Passive cooling, No fans or moving parts
- Redundant power inputs
- Built to IP30 standards



## 112D-POE

- 8x GE RJ45, 4x GE SFP slots
- 8x GE Ports are PoE/PoE+ capable.



## 124D Switch

- 16x GE RJ45, 4x GE SFP slots
  - 8 shared media interfaces (GE RJ45 / GE SFP slots)

# FortiSwitch Product Lineup

Rugged	FS-1xx	FS-2xx	FS-4xx	FS-5xx	FS-1xxx	FS-3xxx
FSR-112D-POE	FS-108E	FS-224E	FS-424D	FS-524D	FS-1024D	FS-3032D
FSR-124D	FS-108E-POE 65W	FS-224E-POE 180W	FS-424D-POE 185W	FS-524D-FPOE 400W	FS-1048D	
	FS-108E-FPOE 130W	FS-224D-FPOE 370W	FS-424D-FPOE 370W	FS-548D	FS-1048E	
	FS-124E	FS-248E	FS-448D	FS-548D-FPOE 750W		
	FS-124E-POE 185W	FS-248E-POE 370W	FS-448D-POE 370W			
	FS-124E-FPOE 370W	FS-248E-FPOE 740W	FS-448D-FPOE 740W			
Rugged L2 Switches	L2 Switches	+ L3, MLAG	+ 10G Uplinks	+ 40G Uplinks	+ 10G Switches	+ 40G Switch

- All POE models support POE and POE+
- FS-5xx POE Power can be increased with second PSU
- FSR-112D-POE POE Power depends on input voltage
  - 44–49V input voltage can support PoE on all ports,
  - 50–57V input voltage can support PoE+ on all ports.
- 1048D is 40x10G and 4x40G
- 1048E is 48x10G and 6x40G or 4x100G



# Security Fabric Integration

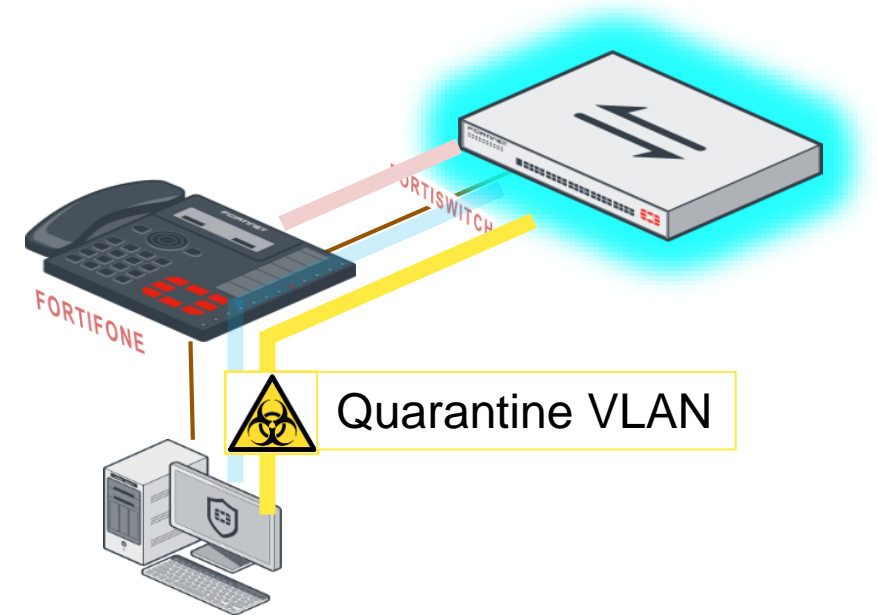
FortiSwitch Controlled by FortiGate

# Host Quarantine

Isolate Host at FortiSwitch Port

## ■ Benefits:

- » Isolate malicious traffic
- » Avoid spread of attacks
- » Allow for remedial action
- » Centrally manage quarantined users



## ■ Host MAC address is moved to Quarantine VLAN

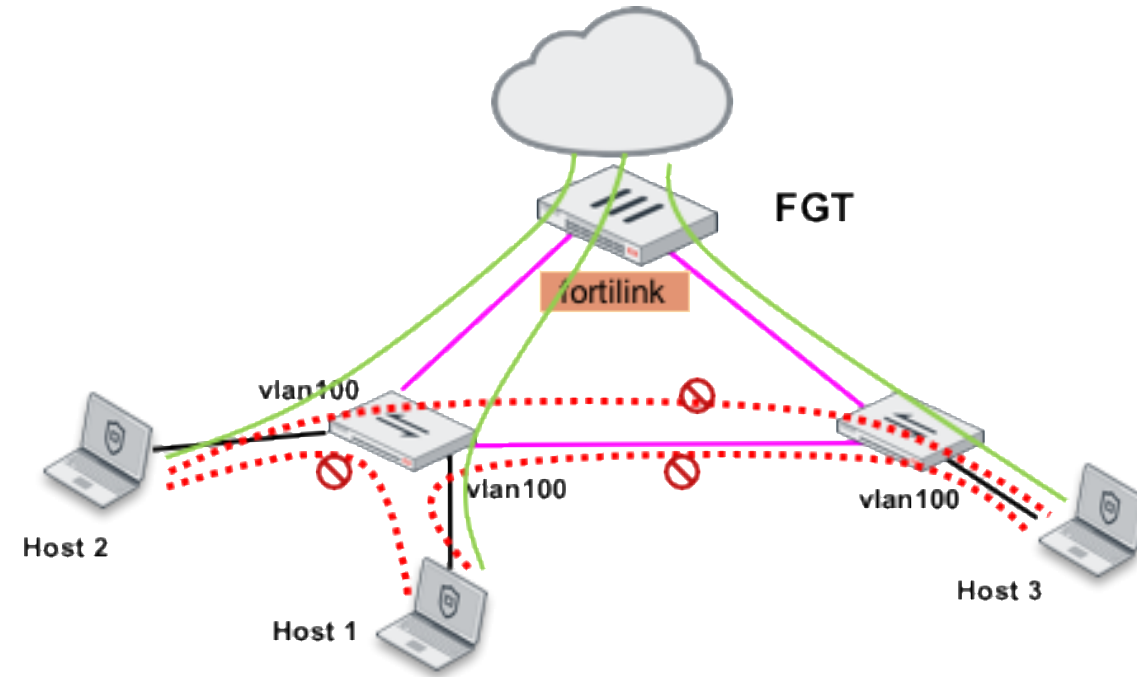
- » Full isolation
- » Captive Portal for remedial actions

# Access VLAN

Isolate the hosts visibility

## ■ Benefits:

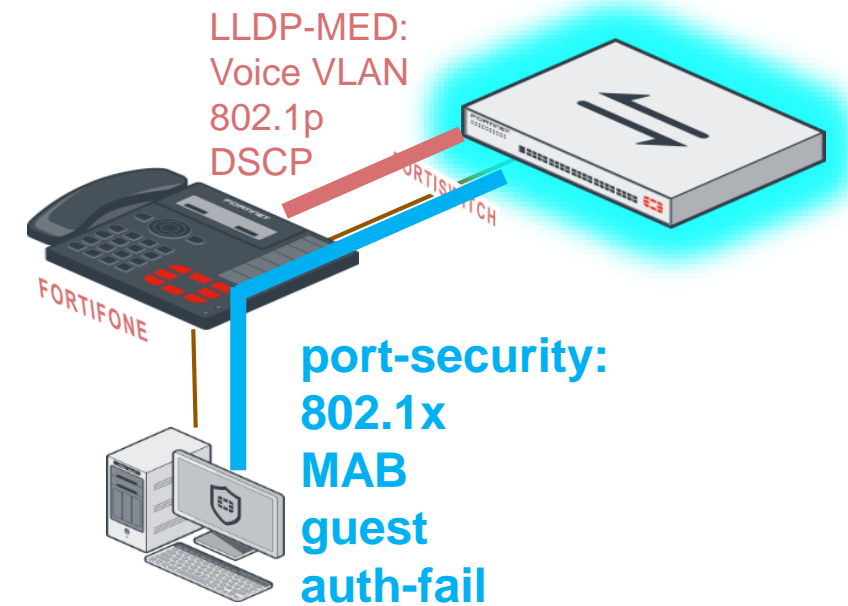
- » Provide extra security to the Access: **block intra-vlan traffic**
- » Hosts are not able to see each other in the same VLAN
- » Host can only communicate with the FGT
- » The FGT implements the allowed access per host or group of hosts



# Access Security and Device Discovery

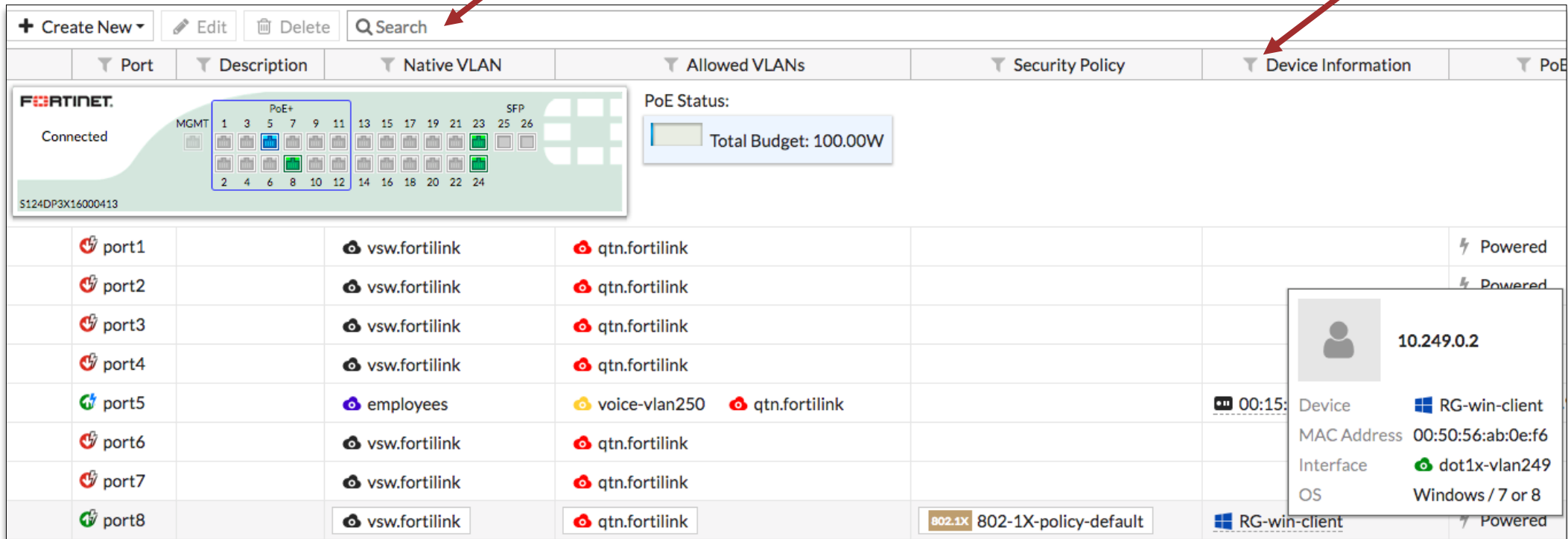
## 802.1x Dynamic VLAN Assignment and LLDP-MED

- **LLDP-MED:** Assign network settings (VLAN, 802.1p and DSCP values) to devices (e.g. IP phones)
  - » no need to manually configure end device
  - » QoS to voice traffic
- **802.1x:** Dynamic VLAN Assignment
  - » flexible access control
  - » multiple hosts on single physical port
  - » enhanced security
  - » combined with LLDP-MED, client and phone share same switch port -> half # ports required



# Device Detection – Per Port Device Visibility

- Allows visibility of MAC address on FSW port
- Easily Searchable!



The screenshot displays the Fortinet FortiGate GUI for port configuration. At the top, there are buttons for '+ Create New', 'Edit', 'Delete', and a 'Search' bar. Below these are tabs for 'Port', 'Description', 'Native VLAN', 'Allowed VLANs', 'Security Policy', 'Device Information', and 'PoE'. The 'Port' tab is active, showing a port configuration for 'port8'. A 'PoE+' status indicator is visible, showing a grid of ports with status icons. A 'PoE Status' box indicates 'Total Budget: 100.00W'. Below the port configuration, a table lists the port details:

Port	Description	Native VLAN	Allowed VLANs	Security Policy	Device Information	PoE
port1		vsw.fortilink	qtn.fortilink			Powered
port2		vsw.fortilink	qtn.fortilink			Powered
port3		vsw.fortilink	qtn.fortilink			
port4		vsw.fortilink	qtn.fortilink			
port5		employees	voice-vlan250 qtn.fortilink		00:15:...	
port6		vsw.fortilink	qtn.fortilink			
port7		vsw.fortilink	qtn.fortilink			
port8		vsw.fortilink	qtn.fortilink	802.1X 802-1X-policy-default	RG-win-client	Powered

A detailed view of the device information for port8 is shown in a pop-up window:

- Device: RG-win-client
- MAC Address: 00:50:56:ab:0e:f6
- Interface: dot1x-vlan249
- OS: Windows / 7 or 8

# Fortinet Single Sign On – FSSO



## ■ Benefits:

- » Tighter security posture
- » User visibility

- User-based firewall policies across the network

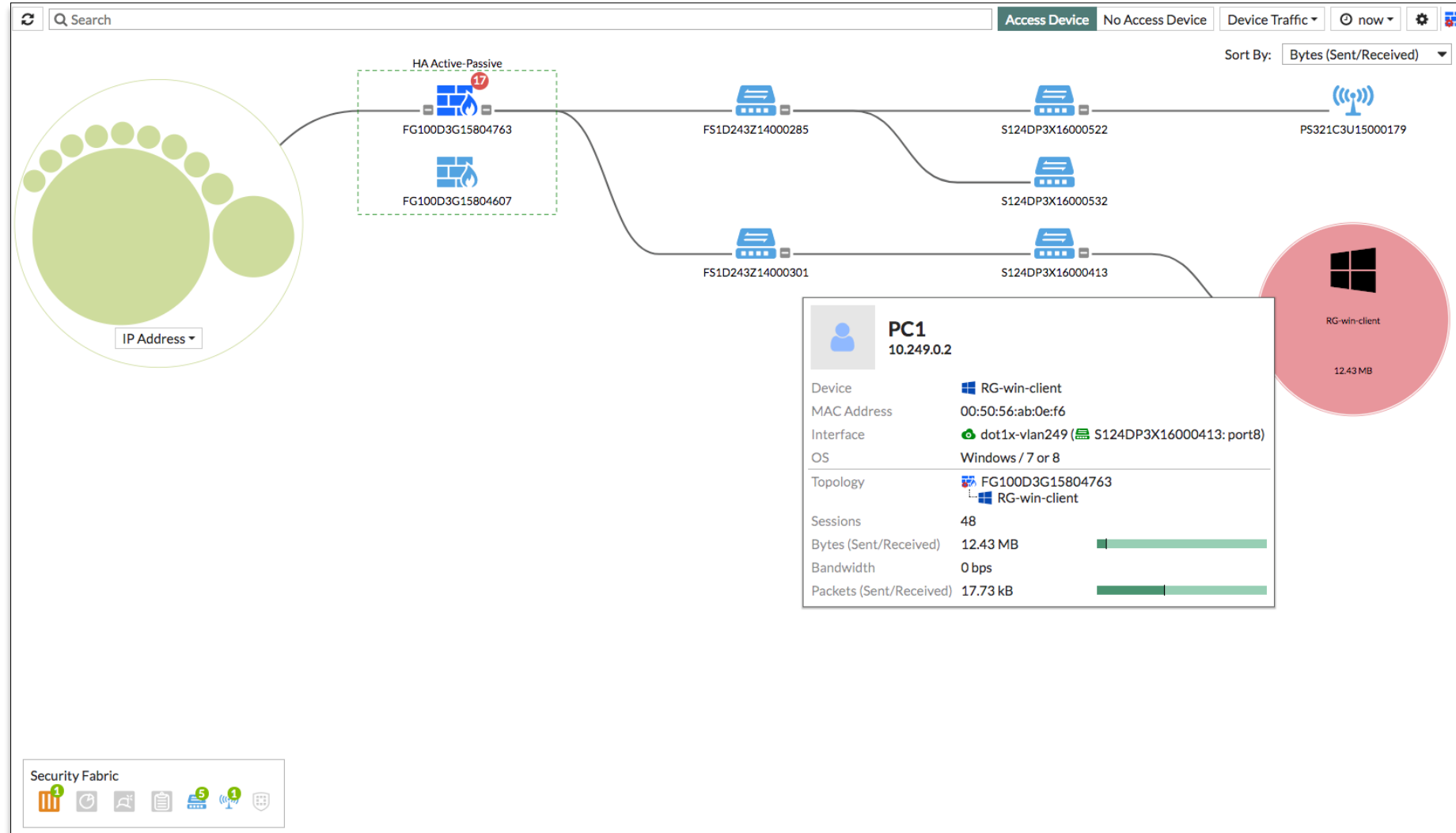
The screenshot shows the Fortinet FSSO Logons interface. On the left is a navigation menu with options like Dashboard, Security Fabric, FortiView, Network, System, Policy & Objects, Security Profiles, VPN, User & Device, WiFi & Switch Controller, Log & Report, and a Monitor section which is expanded to show various monitors including Firewall User Monitor. The main panel displays a table of active sessions. At the top of the table are buttons for Refresh, Deauthenticate, and Show all FSSO Logons, along with a search bar. The table has columns for User Name, User Group, Duration, IP Address, Traffic Volume, and Method. One session is listed for user 'PC1' in the 'fac-sso-group' with a duration of 2 hours 59 minutes 44 seconds, IP address 10.249.0.2, and a traffic volume of 332.43 MB. The method is 'Fortinet Single-Sign-On'.

User Name	User Group	Duration	IP Address	Traffic Volume	Method
PC1	fac-sso-group	2 hours 59 minutes 44 seconds	10.249.0.2	332.43 MB	Fortinet Single-Sign-On

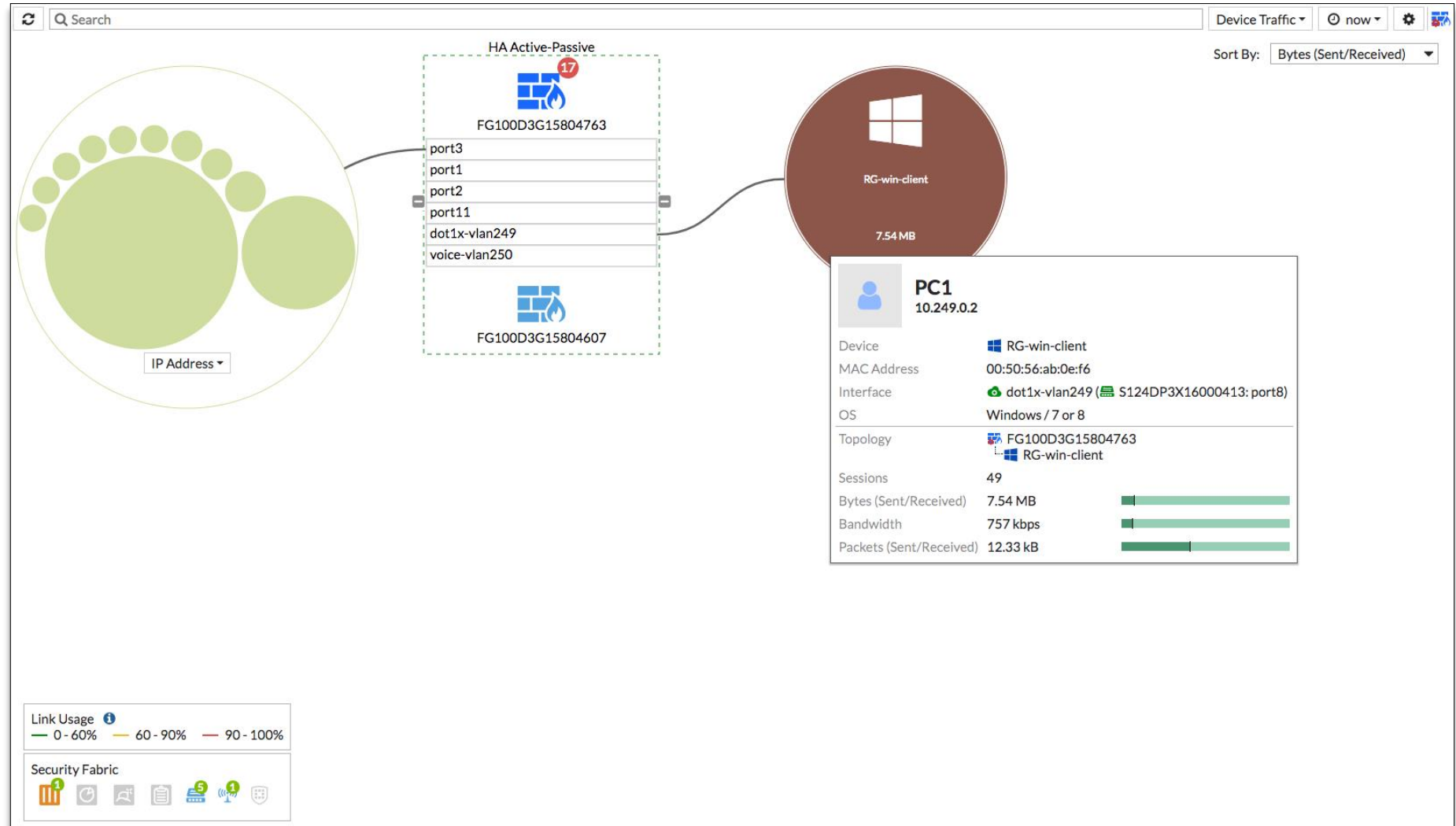


# Security Fabric – Physical Topology

Shows Clients Connected to each FSW

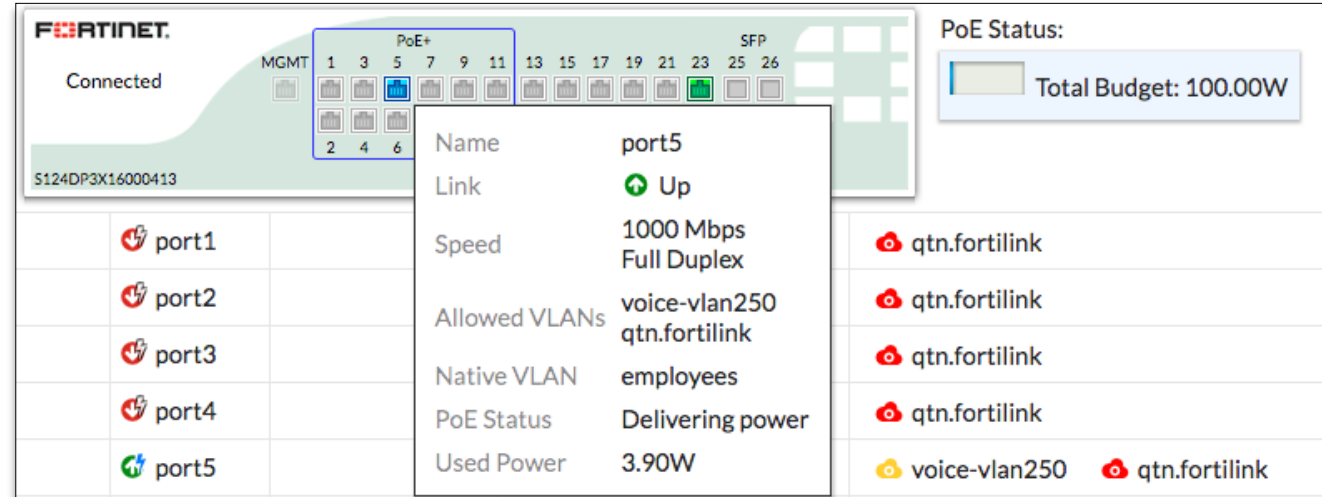


## Shows Clients in each VLAN



# POE Management

- Centralized Control
- POE status can be verified in the GUI
  - » including Total Power Budget



PoE Status:

Total Budget: 100.00W

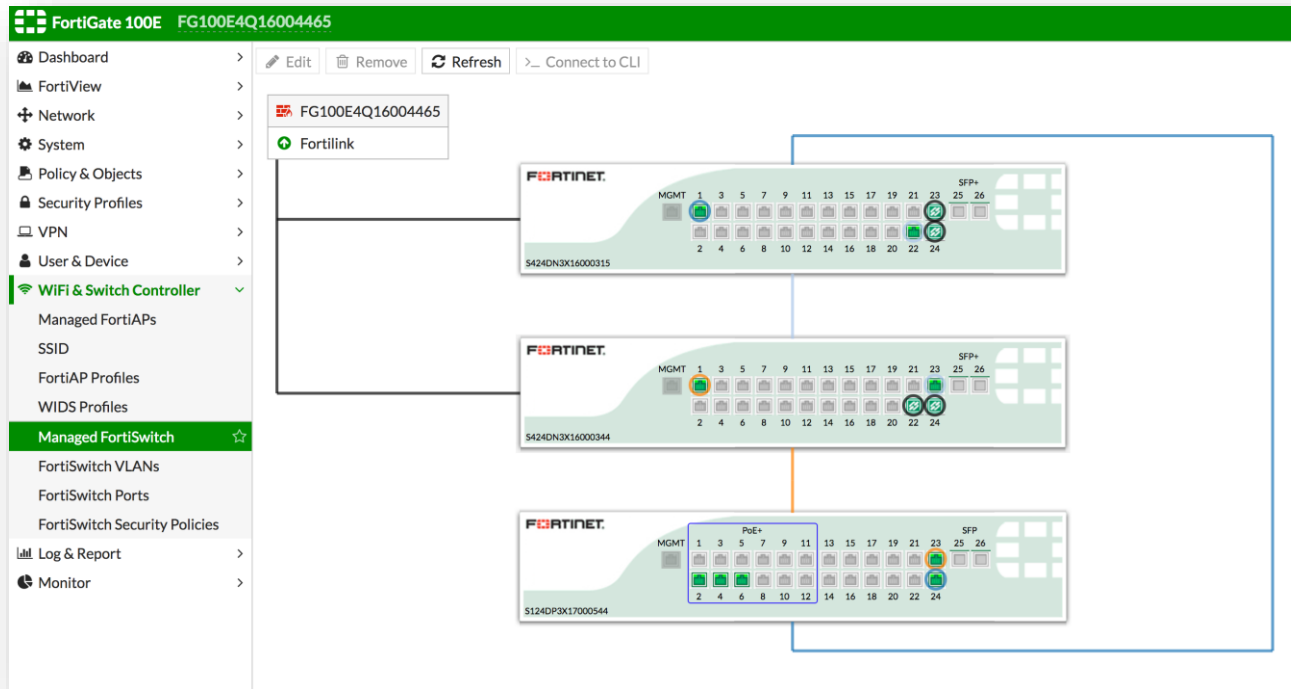
Port	Link	Speed	Allowed VLANs	Native VLAN	PoE Status	Used Power
port1	Up	1000 Mbps Full Duplex	voice-vlan250, qtn.fortilink	employees	Delivering power	3.90W
port2	Up	1000 Mbps Full Duplex	voice-vlan250, qtn.fortilink	employees	Delivering power	3.90W
port3	Up	1000 Mbps Full Duplex	voice-vlan250, qtn.fortilink	employees	Delivering power	3.90W
port4	Up	1000 Mbps Full Duplex	voice-vlan250, qtn.fortilink	employees	Delivering power	3.90W
port5	Up	1000 Mbps Full Duplex	voice-vlan250, qtn.fortilink	employees	Delivering power	3.90W

Port	Description	Native VLAN	Allowed VLANs	Security Policy	Device Information	PoE	Bytes (Sent/Received)
port1		vsw.fortilink	qtn.fortilink			Powered	0 B
port2		vsw.fortilink	qtn.fortilink			Powered	0 B
port3		vsw.fortilink	qtn.fortilink			Powered	0 B
port4		vsw.fortilink	qtn.fortilink			Powered	0 B
port5		employees	voice-vlan250 qtn.fortilink		00:15:65:83:cb:16	Powered 3.90W	160.32 MB
port6		vsw.fortilink	qtn.fortilink			Powered	0 B
port7		vsw.fortilink	qtn.fortilink			Powered	0 B
port8		vsw.fortilink	qtn.fortilink	802.1X 802-1X-policy-default	RG-win-client	Powered	525.13 MB

# FortiLink

# FortiLink – Secure Access and Management

## FortiGate Switch Management



- » **Fortilink** protocol for secure management
- » Visibility into port speed/status
- » POE status and management
- » Centrally manage VLANs
- » Apply security policy
- » Authenticate clients centrally via 802.1x or captive portal

# FortiLink: Under the Hood

FortiOS 6.0.0 and FortiSwitchOS 3.6.6



# FortiLink Requirements – FortiGate

Functionality	5.4.1 and later
All FSW directly connected	only one required, multiple possible with hw- or sw-switch
# of interfaces on FGT enabled for FortiLink	one (multi-interface supported without GUI)
interface type on FGT	physical, aggregate, hw- or sw-switch
FGT mode	interface

# What's running on FortiLink?

- FortiLink Heartbeat
- LLDP → FSW discovery
- CAPWAP → configuration commands, software upgrade
- NTP → time sync with FGT
- HTTPS → config and diag commands via REST API
- FSW InterSwitch Link

# Fortilink Port Assignment

FortiSwitch	Default Ports for Fortilink * any port can be used if manually configured
FS-108E-POE, FS-108E, FS-108E-FPOE	9 and 10
FSR-112D-POE	5, 6, 7, 8, 9, 10, 11 and 12
FS-224E-POE	21, 22, 23 and 24
FS-124E, FS-124E-POE	23, 24, 25 and 26
FS-224D-FPOE, FS-224E, FS-224E-POE	21, 22, 23, 24, 25, 26, 27 and 28
FS-248E, FS-248E-POE, FS-248E-FPOE FS-448D, FS-448D-FPOE, FS-448D-POE	45, 46, 47, 48, 49, 50, 51 and 52
FS-424D, FS-424D-FPOE, FS-424D-POE	23, 24, 25 and 26
FS-524D, FS-524D-FPOE	21, 22, 23, 24, 25, 26, 27, 28, 29 and 30
FS-548D-FPOE, FS-548D	45, 46, 47, 48, 49, 50, 51, 52, 53 and 54
FS-1024D, FS-1048D, FS-3032D	all ports

# FOS 5.4.3 and later – Max number of FSW per FGT

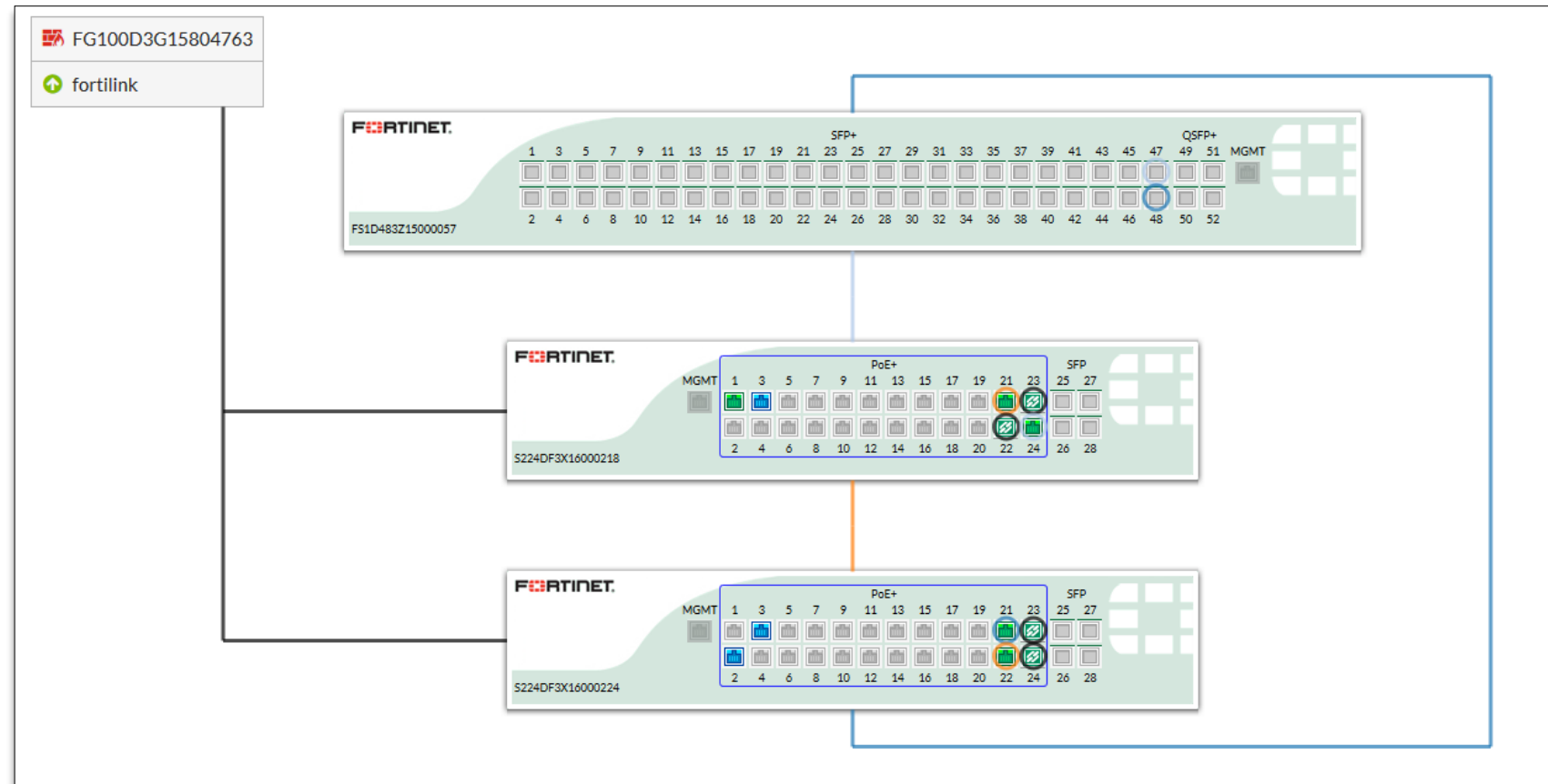
FGT Model	Max number of FSW
up to FG-98D / VM01	8
FG-100D to FG-280D / VM02	24
FG-300D to FG-500D	48
FG-600D to FG-900D / VM04	64
FG-1000D to FG-2xxxE	128
FG-3xxx and above / VM08	300

# It's easy to control FSW 😊

Adding more ports to FortiGate

# Controlling FortiSwitch with FortiGate

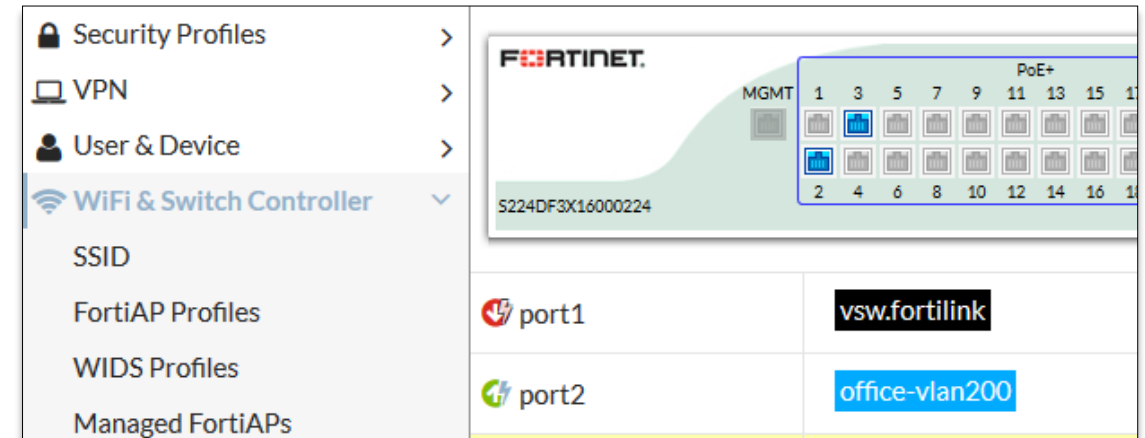
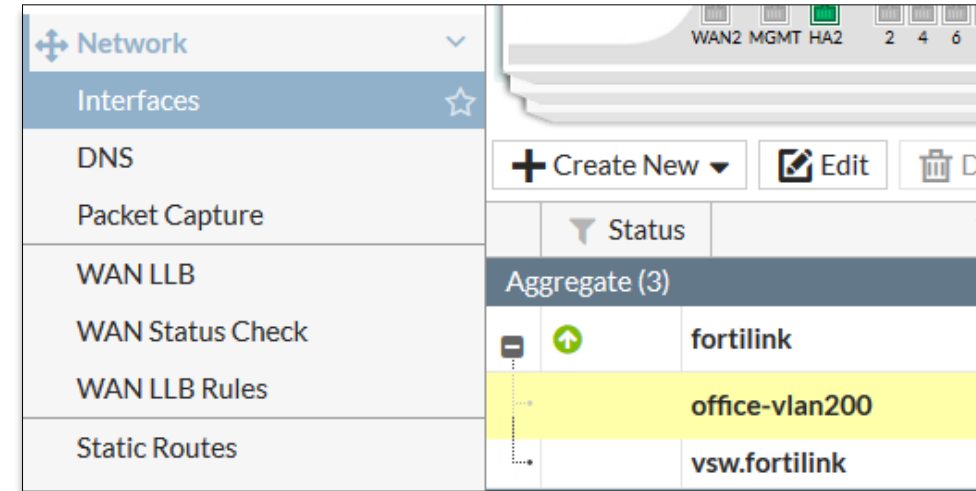
1. Configure interface for Fortilink
2. Connect FSW





# VLAN Assignment

1. Create VLAN interface under interface dedicated to FortiSwitch
2. Assign to FortiSwitch ports



# Ready to apply FortiGate Top Class Security

- Security Policy

FortiGate 100D FG-100D-HA1				
Dashboard	☆	+ Create New	✎ Edit	🗑 Delete
FortiView	>	🔍 Policy Lookup		
Network	>	🔍 Search		
System	>			
Policy & Objects	▼			
IPv4 Policy	☆			
		Seq.#	🔍 Name	🔍 From
		1	office-vlan200-to-internet	📶 office-vlan200 (fortilink)
		2		📶 lan
		3	Implicit Deny	📶 wan1
				📶 wan1
				📶 any
				📶 any

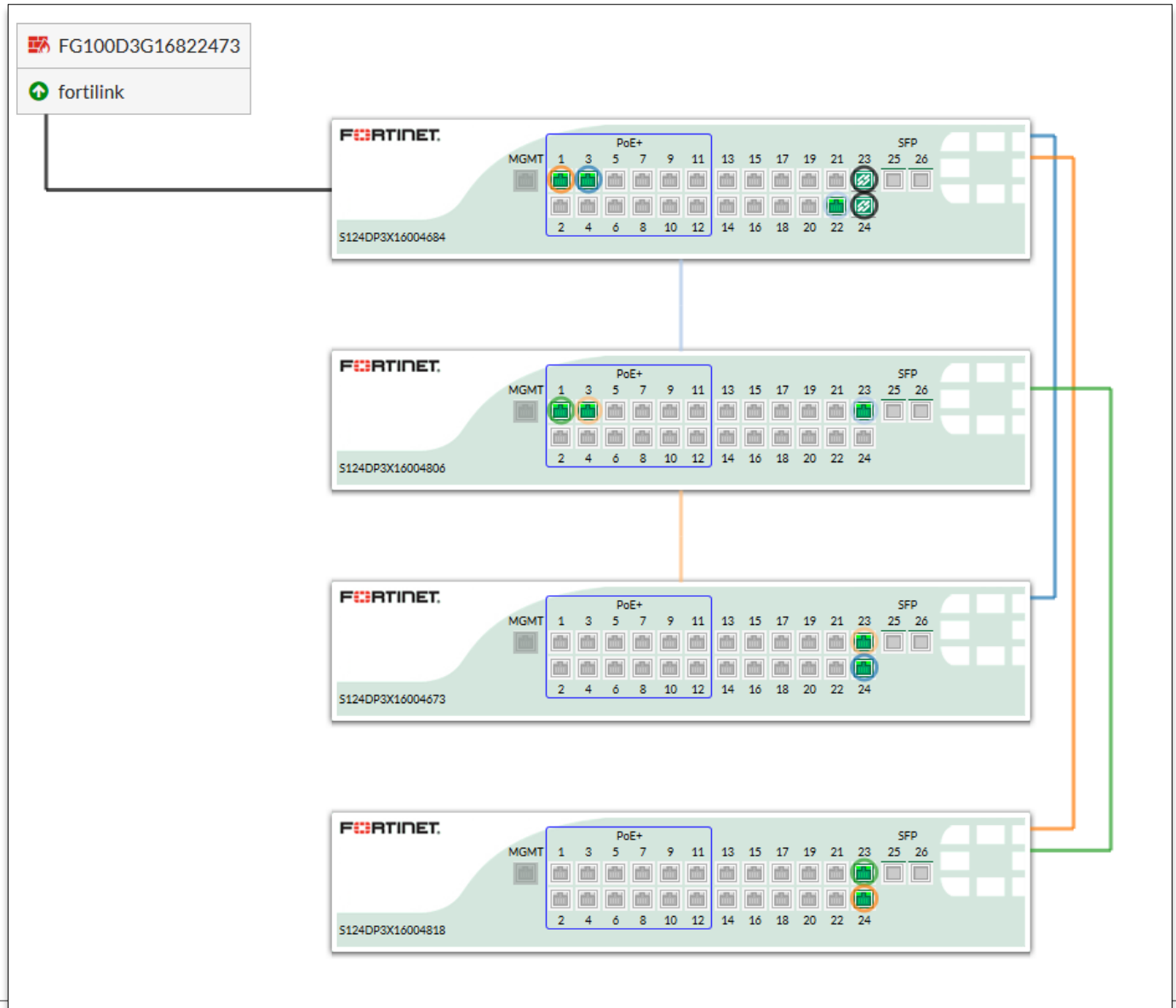
# FortiLink Stacking

## High Port Density with Ease of Management

- Single IP for Management
  - » FortiGate is the switch controller
  
- Wide Range of solutions
  - » From SMB/Retail to Data Center
    - 8 ports with single FortiSwitch to
    - more than a thousand ports with multiple FortiSwitches
  - » Any combination of Gig or 10G Switches
  - » Multiple topologies supported
  
- Collapsed layers
  - » Physically 2 layers (FortiGate-Routing/Security and FortiSwitch-Switching)
  - » Logically single layer

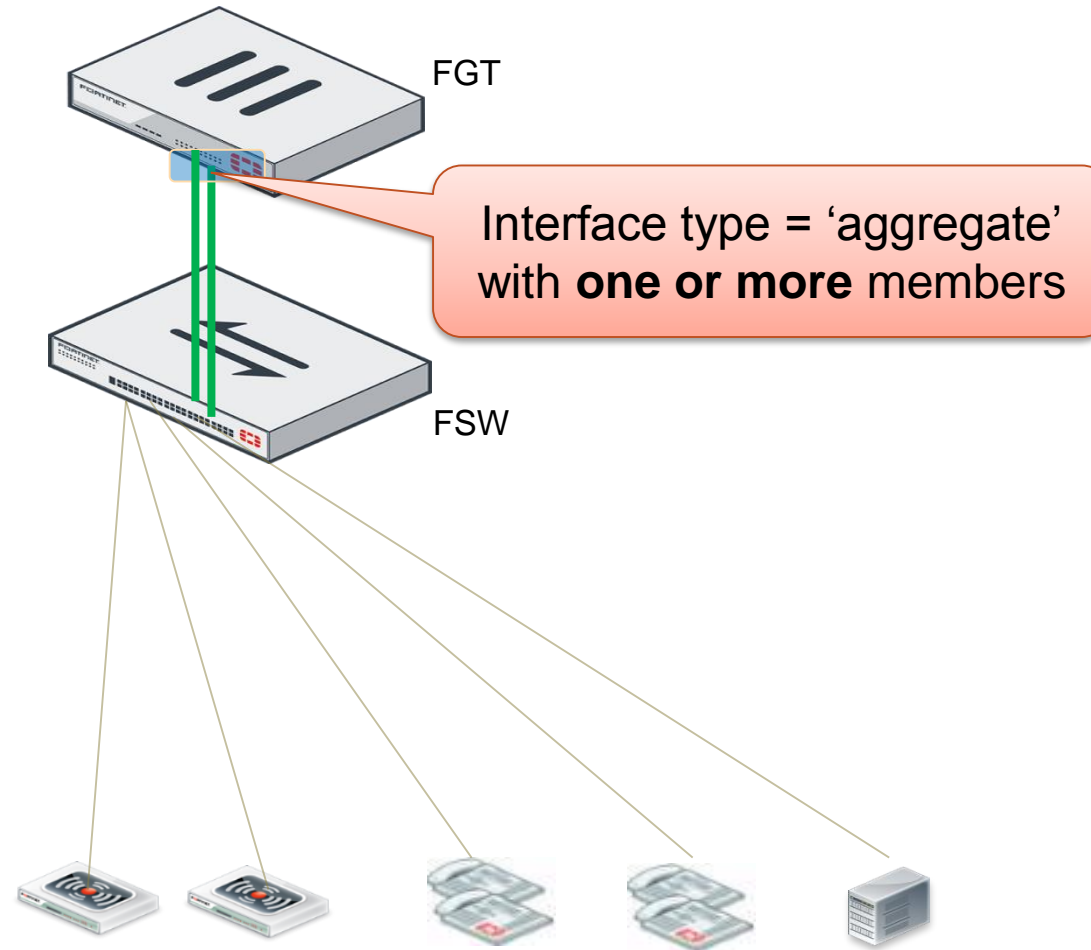
# FortiSwitch Stacking

- All ports in a single pane of glass



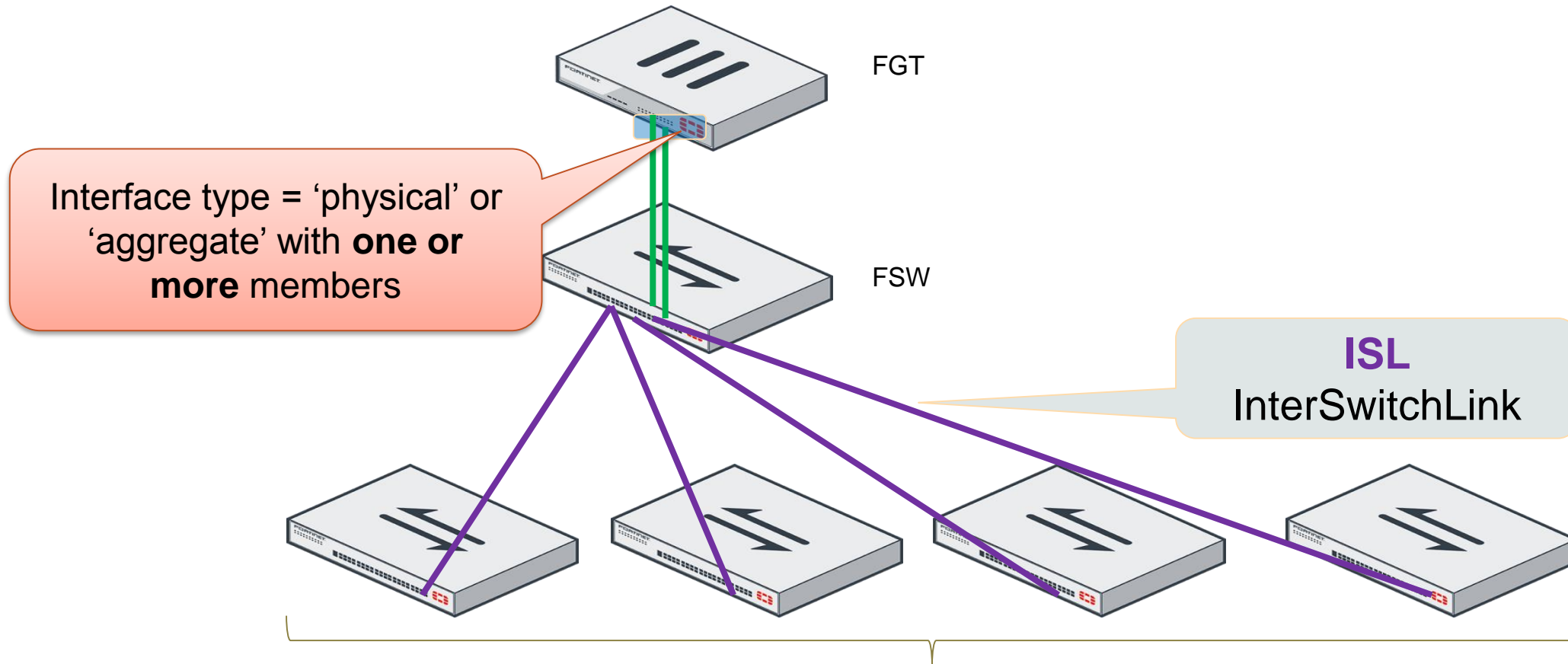
# FortiLink Supported Topologies

# FortiLink Single FSW



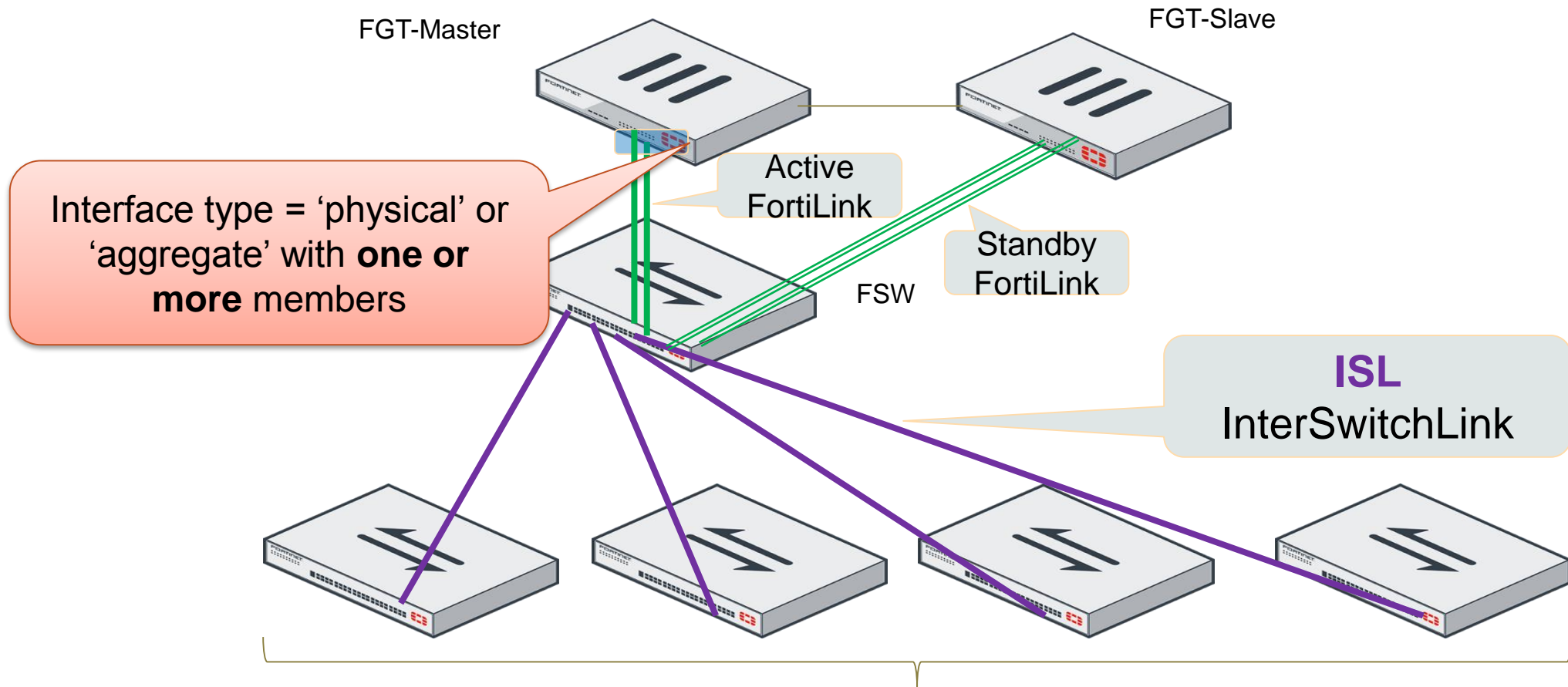


# FortiGate and Multiple Switches (Star)



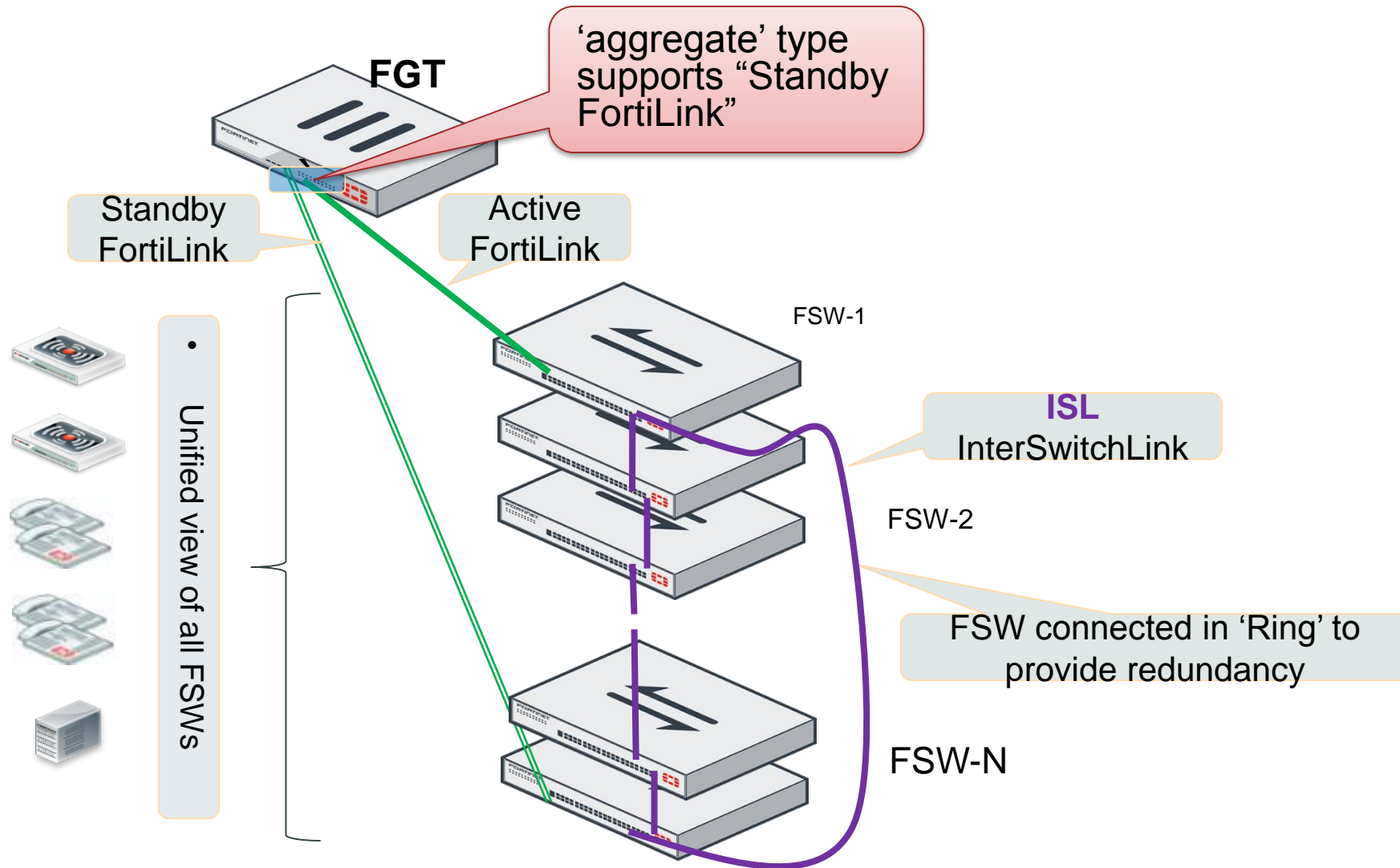
- A port can be member of multiple vlans (native-vlan + number of allowed-vlans)

# FGT HA Pair and Multiple Switches (Star)

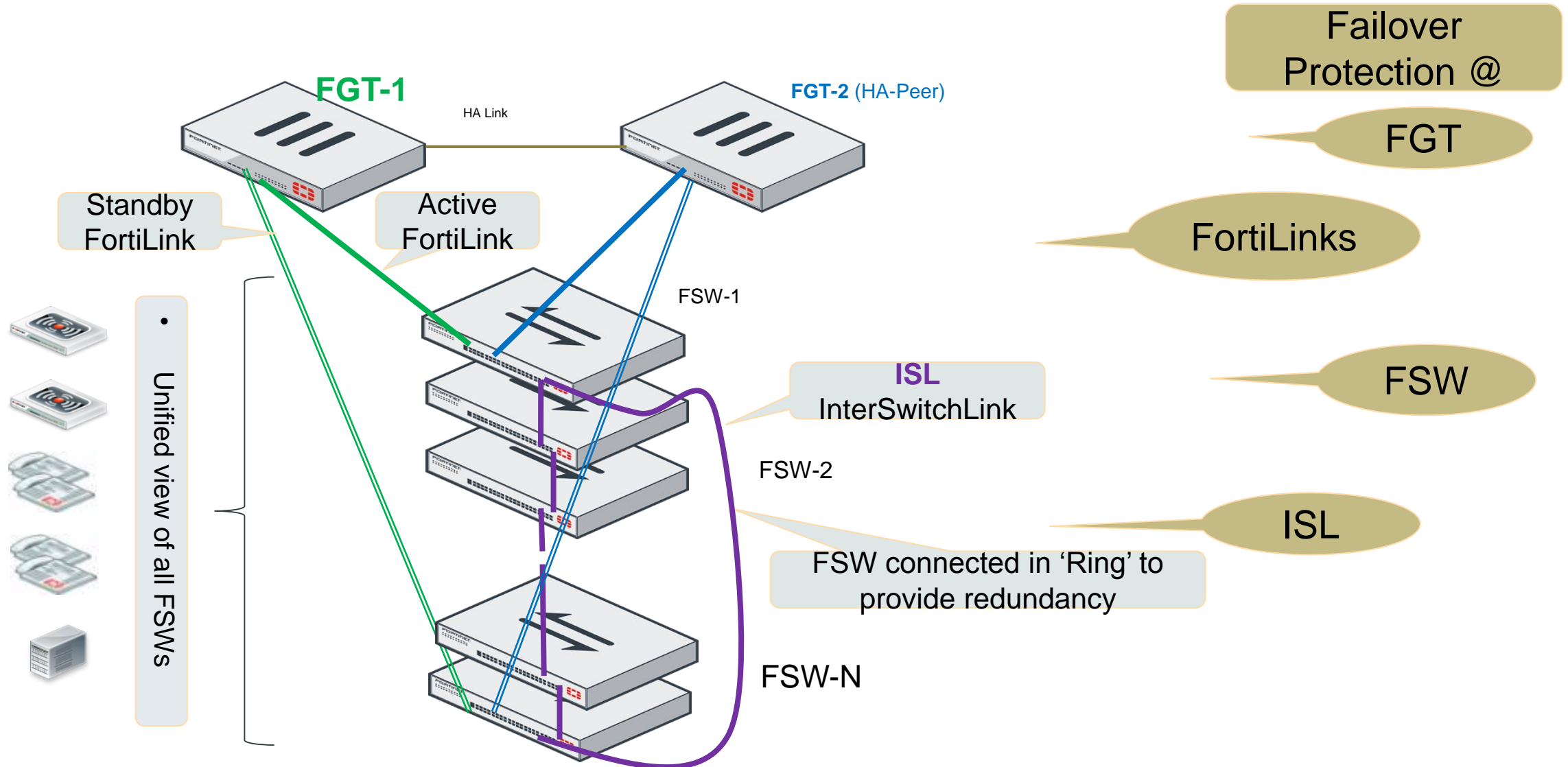


- A port can be member of multiple vlans (native-vlan + number of allowed-vlans)

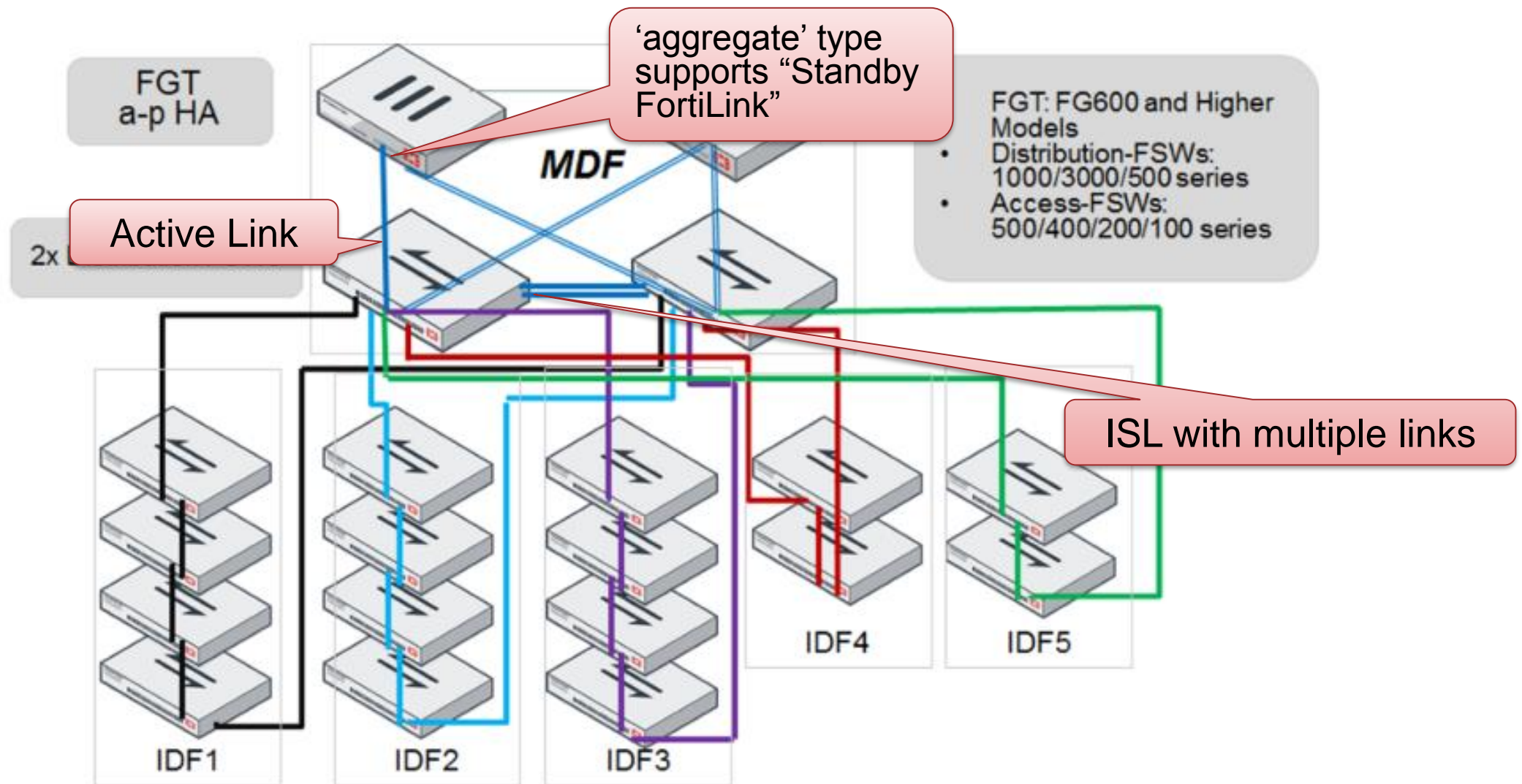
# FortiGate and Multiple Switches (Ring)



# FGT HA Pair and Multiple Switches (Ring)



# Enterprise/Office Closet



# Enterprise with MCLAG

## FortiLink

FG-100E-1  
active

FGT interface type 'aggregate' supports Active/Active FortiLink with MCLAG on FSW (max physical members platform dependent)

HA 1

Active Links

fortilink

fortilink

MCLAG

FS-424D-1

FS-424D-2

MCLAG-ICL with multiple links

MCLAG

FS-124D-POE

access FSW is dual-homed



MCLAG



FortiLink FGT-Distribution FSW



FortiLink Access

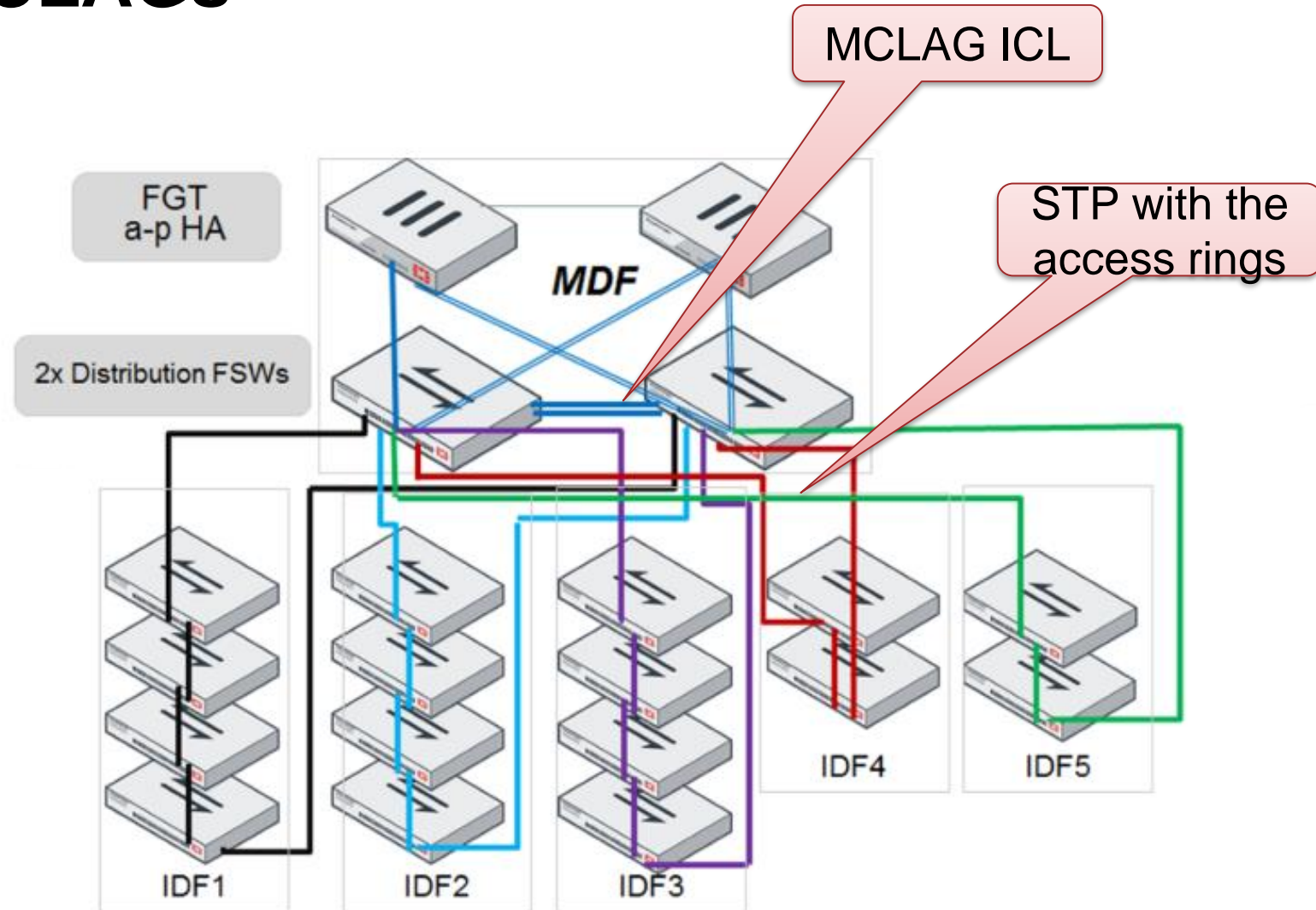


FortiLink Access



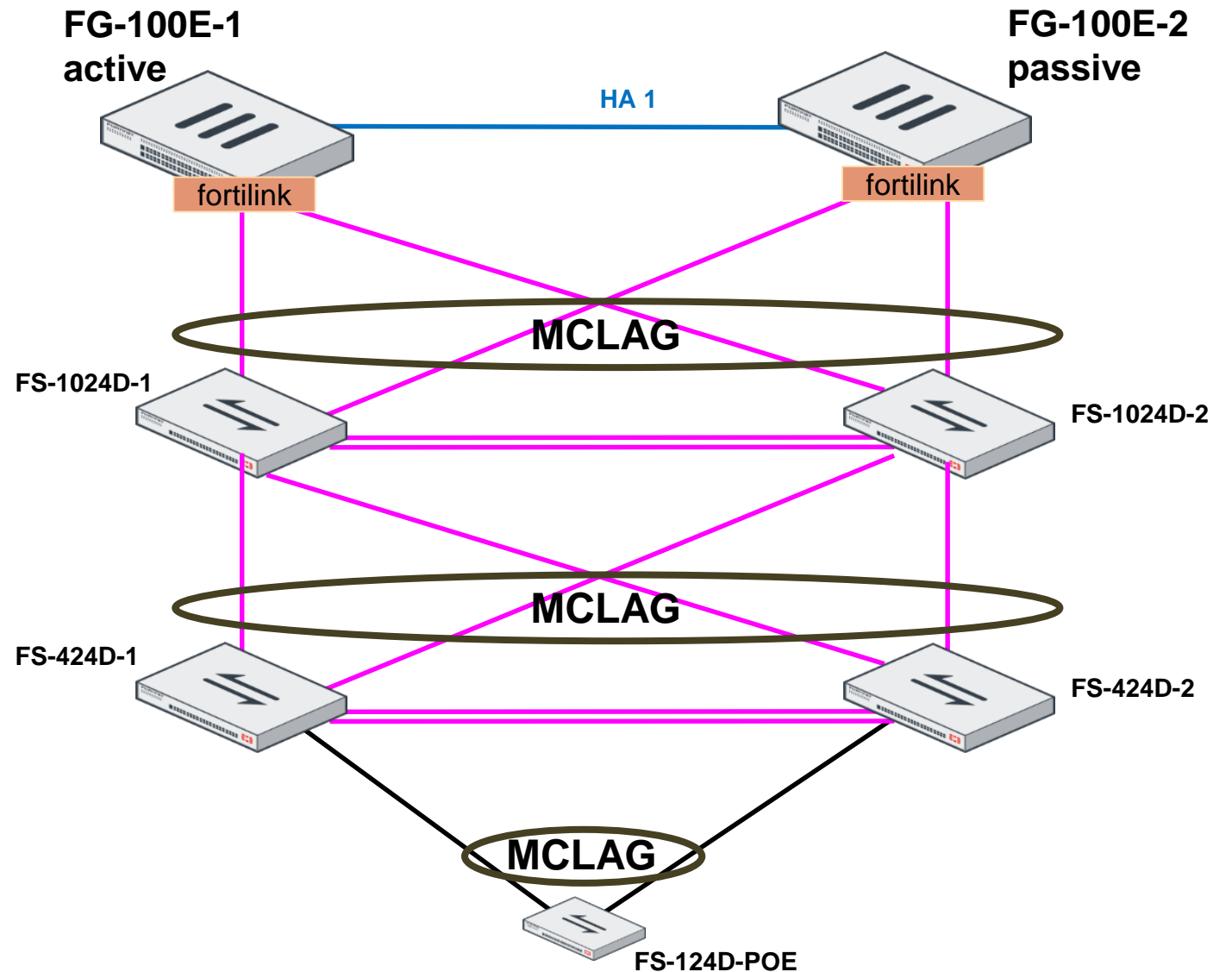
# STP supported in MCLAGs

- Distribution FSW will implement MCLAG and MCLAG ICL
- Automatic STP configuration with the Access rings
- Both distribution FSWs will be seen as one STP entity, and both present same root MAC address and priority



# Support for 2<sup>nd</sup>-Tier MCLAG

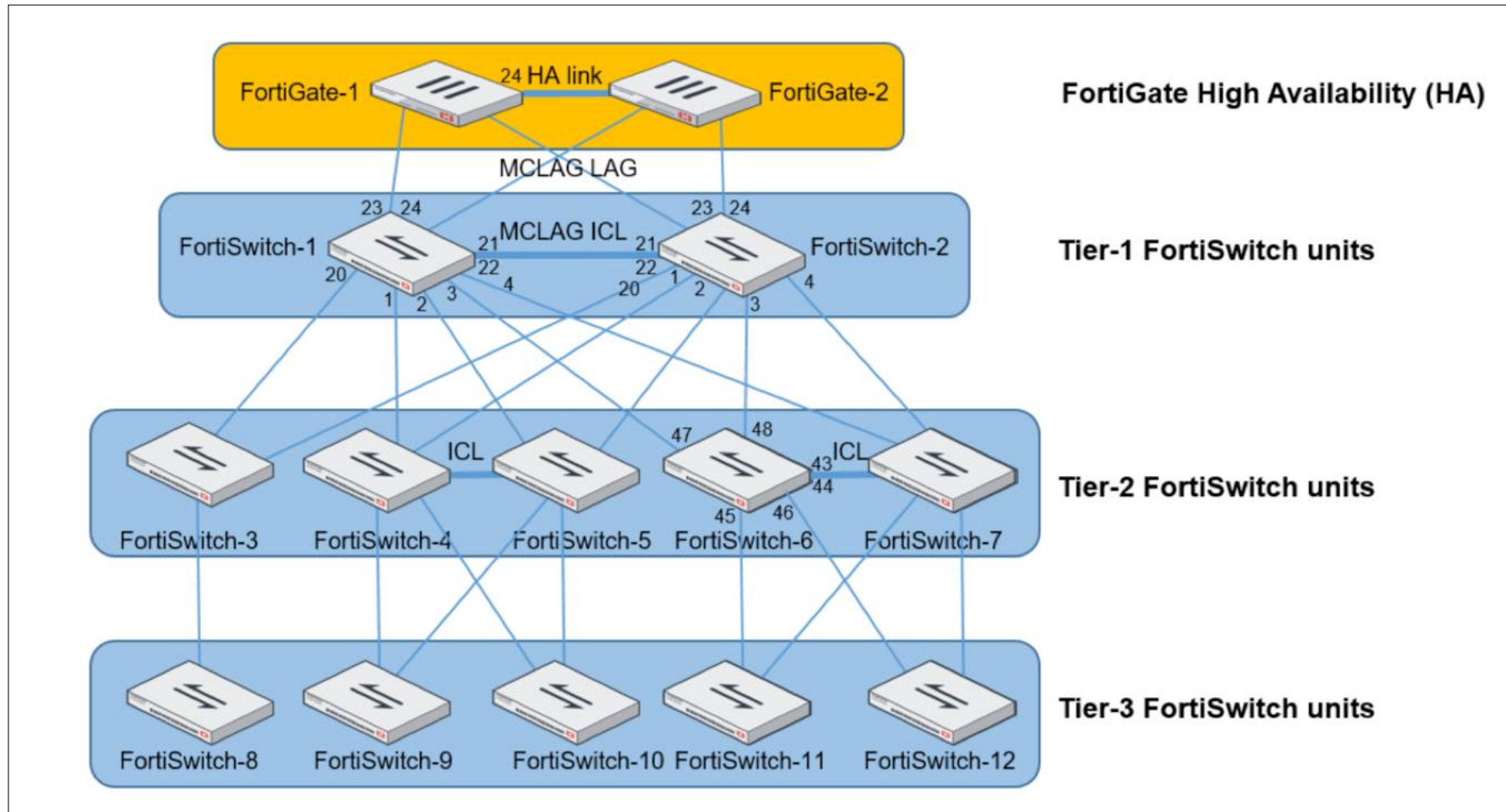
- More scalable design
- Faster failover than ring with STP
- Switch redundancy for server connectivity
- Top of rack/floor switch redundancy





# Large Scale Deployment

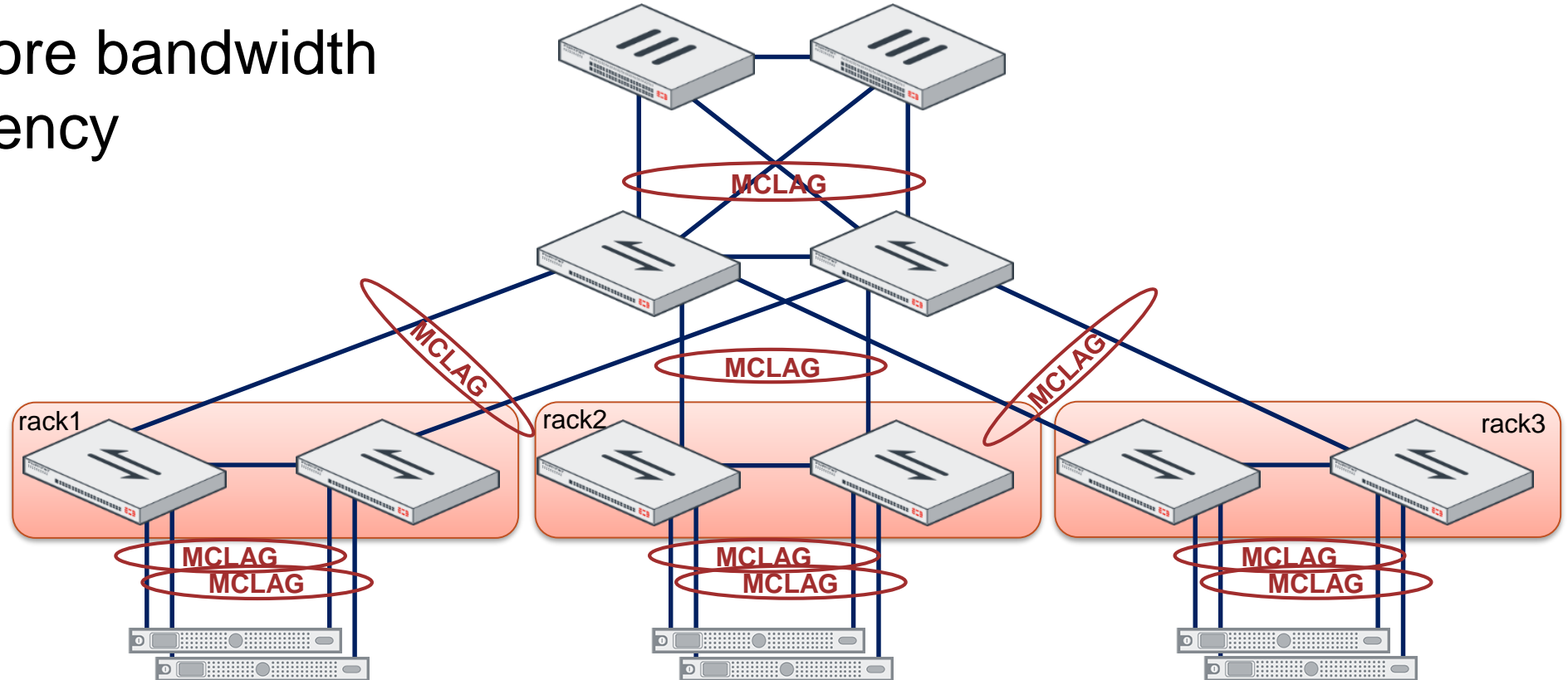
FortiLink



# Scalable

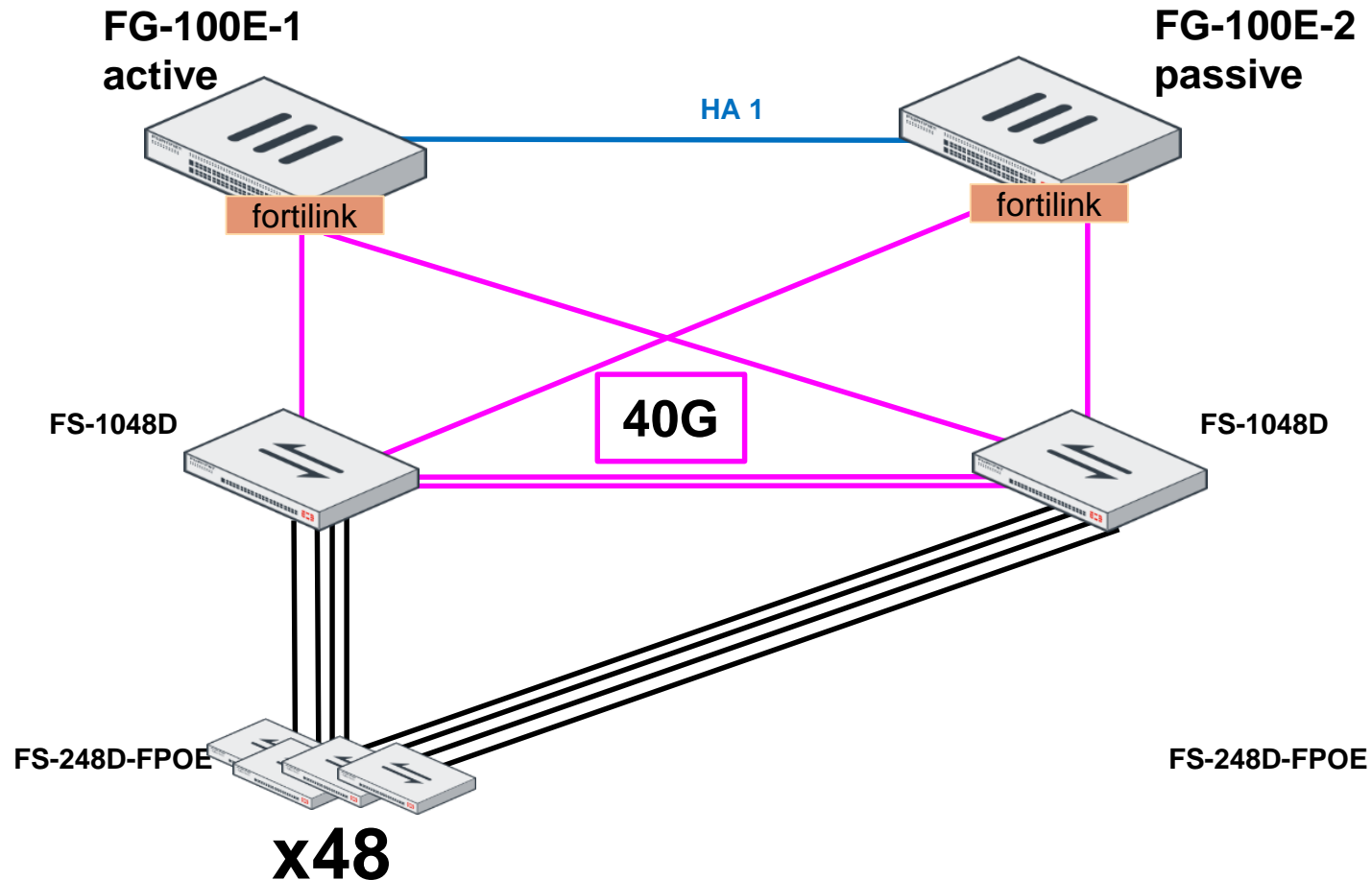
## 2<sup>nd</sup>-tier MCLAG – Link and Switch Redundancy

- Allows more bandwidth and resiliency



# Large Scale Deployment

FortiLink

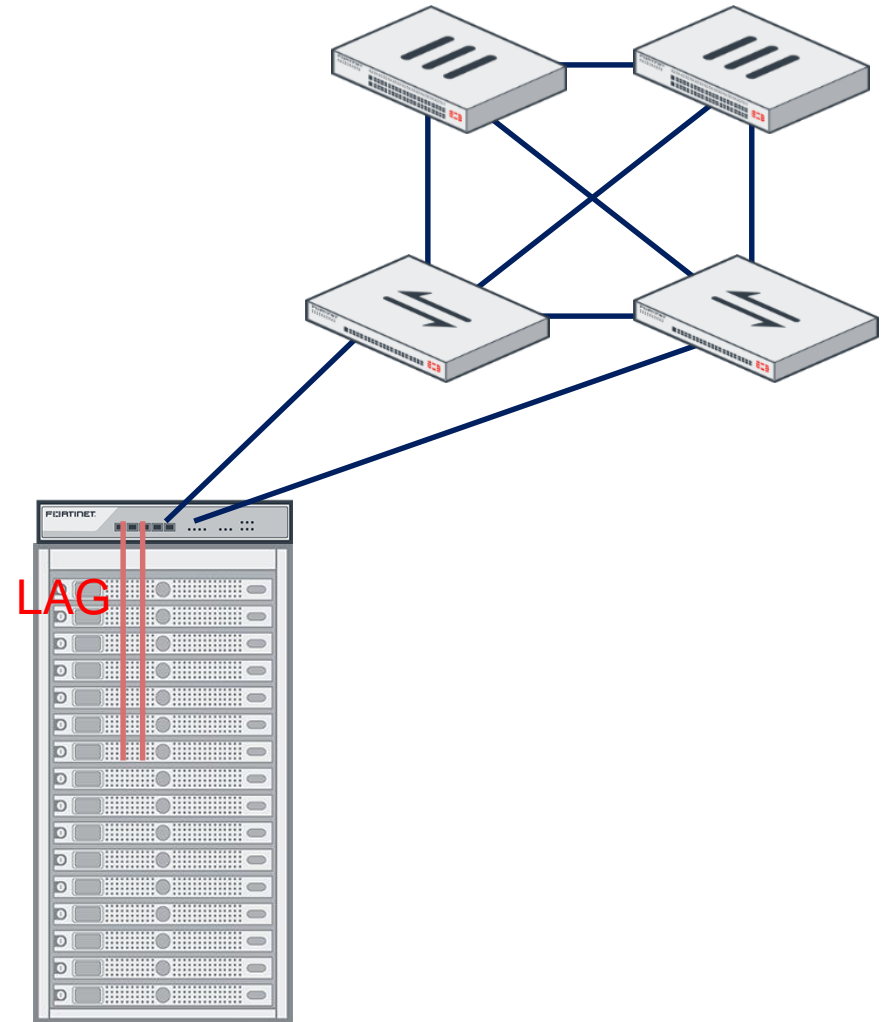


**Total number of ports:  $48 \times 48 = 2304$**

# Additional FortiLink Functionality

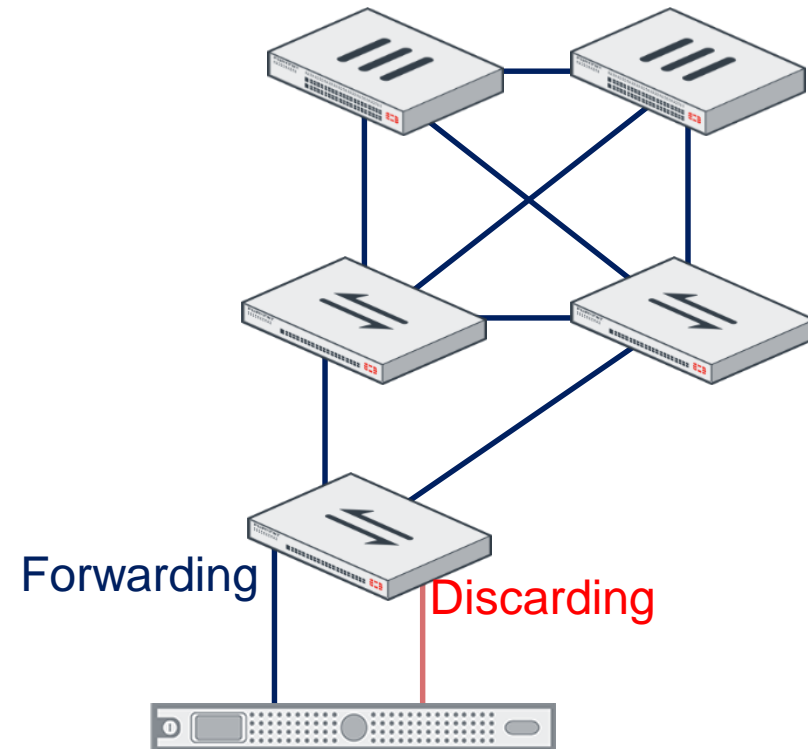
# 802.3ad LAG User Ports

- Allows more bandwidth and resiliency in the connection to servers in the data center top of the rack



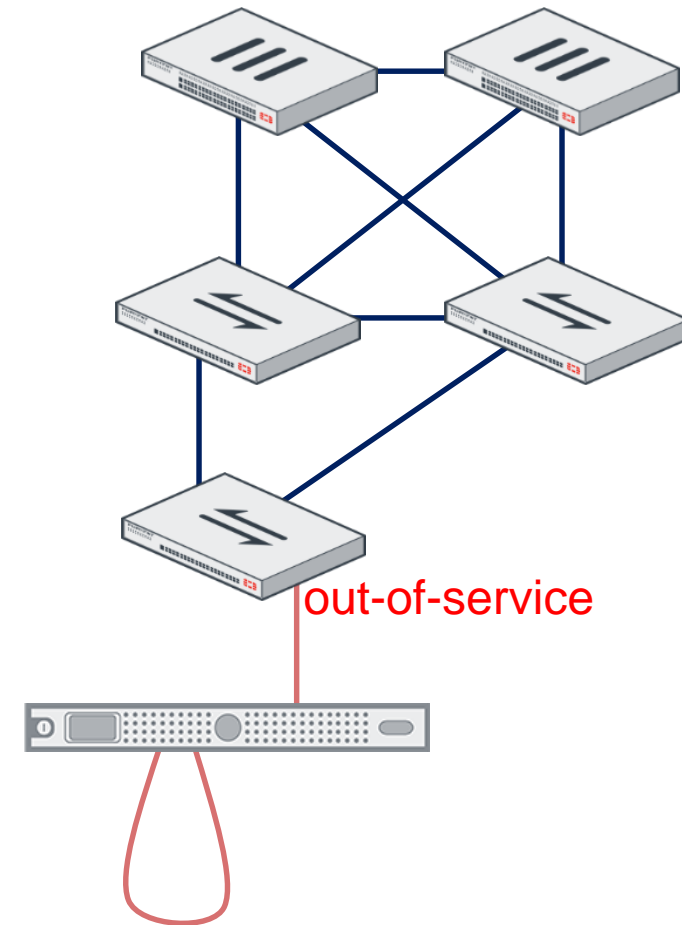
# Loop Protection – Spanning Tree

- Protection against loops in L2 environment



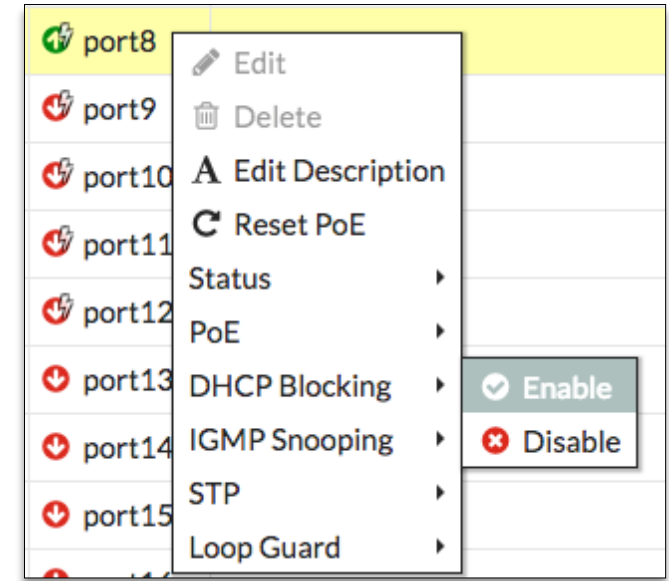
# Loop Protection – LoopGuard

- If a port detects a loop downstream, system takes the port out of service to protect the overall network
  - » complements STP



# DHCP Snooping

- DHCP untrusted/trusted
  - » block/allow DHCP offers from port to the network
  - » protect against rogue DHCP server
  - » easily enabled on the FSW port list



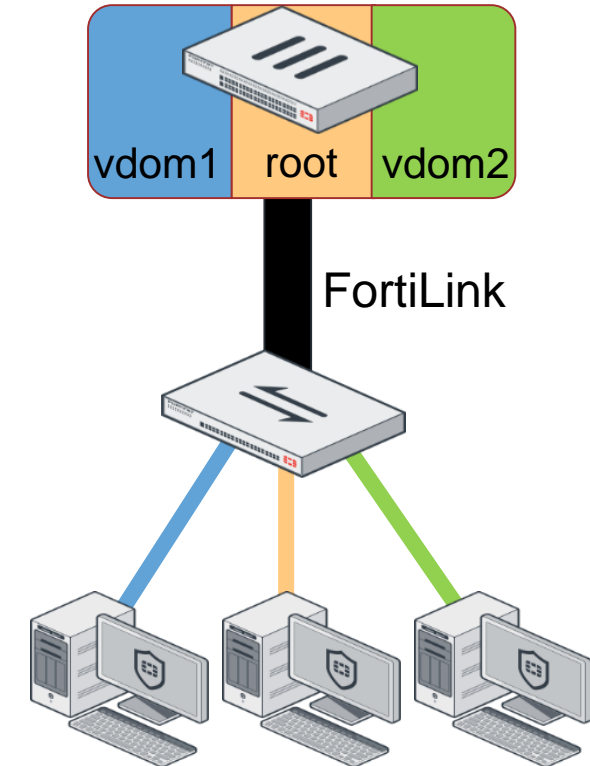


# New features

# Multi Tenancy

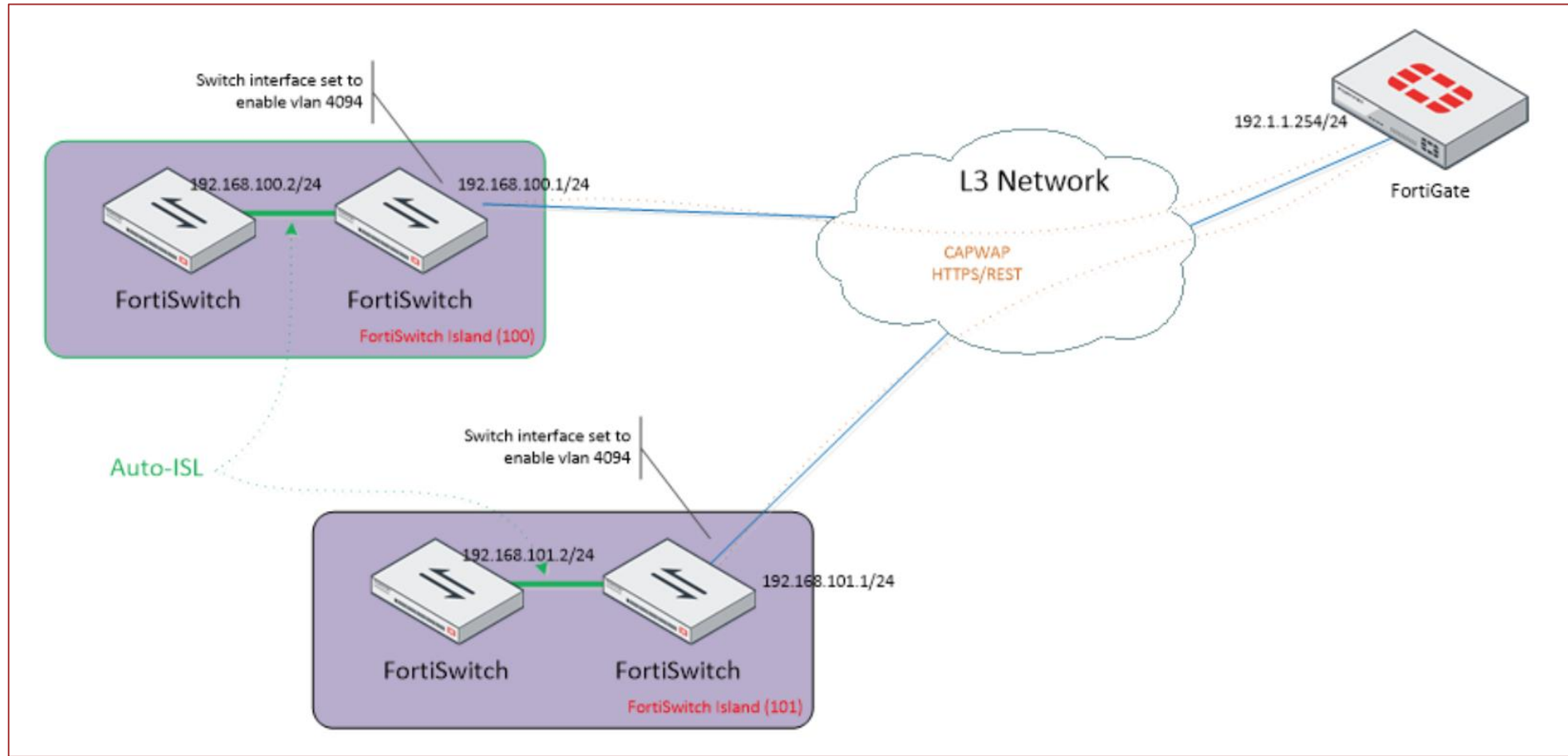
Sharing FSW ports with VDOMs

- Flexibility in multi tenant solutions
- Ports of the same FSW can be shared between VDOMs



# FortiLink over L3

FSW is controlled by FGT From Anywhere in the World!

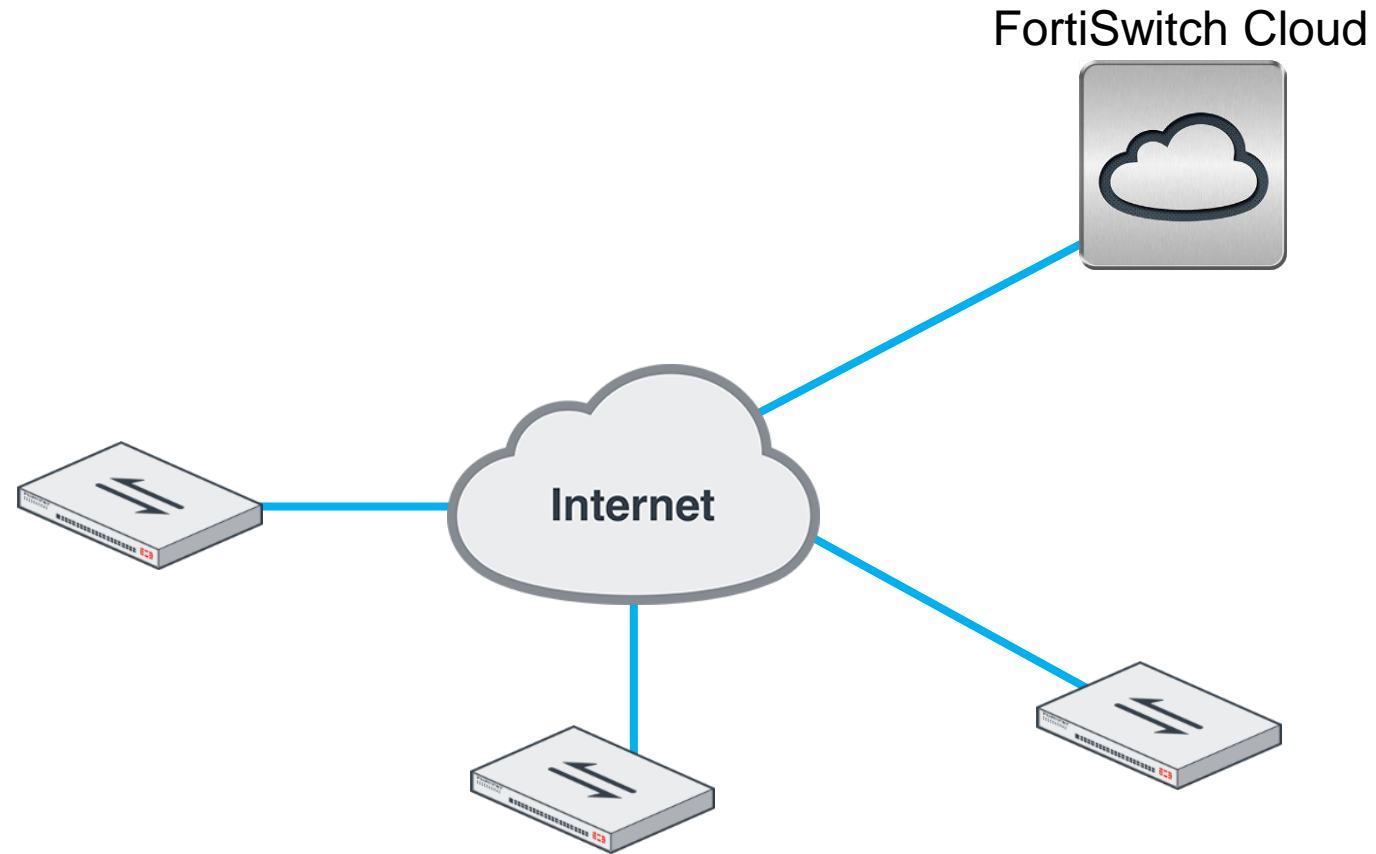


# Feature Support

Feature	FortiLink (direct L2 connection)	FortiLink over L3
Centralized Configuration	✓	✓
Centralized Firmware Management	✓	✓
LAG support for FortiLink Connection	✓	✓
802.1x Authentication (Port-based, MAC-based, MAB)	✓	✓
Host Quarantine on Switch Port	✓	✓
Device Detection	✓	Prototype
Support FortiLink FortiGate in HA Cluster	✓	✓
Active-Active Split MCLAG from FortiGate to FortiSwitch	✓	
Access VLAN	✓	
DHCP Server on VLAN defined on FGT	✓	

# FortiSwitch Cloud

Standalone FSW Central Management Solution



# FortiSwitch Cloud Licensing model

Feature	Free	License
Dashboard	✓	✓
Config restore/backup	✓	✓
Firmware Upgrade	✓	✓
POE enable/disable	✓	✓
Interface List	✓	✓
VLAN Configuration	✓	✓
Device CLI / GUI Access		✓
Monitoring (stats/logs/device)		✓
Topology View		✓
Auditing		✓
Configuration Cloud Storage		✓
Configuration Templates		✓